Alles Compi

Jürgen Hendrik

emo-essen.de

17. Sep 2013

Inhaltsverzeichnis

Inhaltsverzeichnis

Zum Kurs

Termine

Zeitpunkt	Titel
17.09.2013	Das Internet
24.09.2013	Teil 1 Forts. und Fragen
01.10.2013	Installationsparty
08.10.2013	Open Source Programme

Zum Kurs

Termine

Zeitpunkt	Titel
17.09.2013	Das Internet
24.09.2013	Teil 1 Forts. und Fragen
01.10.2013	Installationsparty
08.10.2013	Open Source Programme

Inhalte

- Wie funktioniert das Internet
- Internet für Organisationen ?
- Computer, Software, Betriebssysteme ?
- Freie Software ?

Zum Kurs

Termine

Zeitpunkt	Titel
17.09.2013	Das Internet
24.09.2013	Teil 1 Forts. und Fragen
01.10.2013	Installationsparty
08.10.2013	Open Source Programme

Inhalte

- Wie funktioniert das Internet
- Internet für Organisationen ?
- Computer, Software, Betriebssysteme ?
- Freie Software ?
- Fragen und Ausprobieren

Alles Compi - Teil 1

Internet Schlüsseltechnologien

Hendrik Langer

emo-essen.de

17. Sep 2013

Aus: WIE DAS INTERNET FUNKTIONIERT – Eine Anleitung für Entscheidungsträger und Interessierte
https://digitalegesellschaft.de/wp-content/uploads/2012/04/digiges_wie_das_internet_funktioniert.pdf

Inhaltsverzeichnis

Das Internet

Ein Netzwerk aus Computer-Netzwerken

Das Internet

Ein Netzwerk aus Computer-Netzwerken

- Netzwerk: Verbindung von Computern

Das Internet

Ein Netzwerk aus Computer-Netzwerken

- Netzwerk: Verbindung von Computern
- $\Rightarrow$ Internet: (weltweite) Verbindung von Netzwerken

Das Internet

Ein Netzwerk aus Computer-Netzwerken

- Netzwerk: Verbindung von Computern
- $\Rightarrow$ Internet: (weltweite) Verbindung von Netzwerken
- gemeinsame Sprache: Internet Protocol (IP)

Das Internet

Ein Netzwerk aus Computer-Netzwerken

- Netzwerk: Verbindung von Computern
- $\Rightarrow$ Internet: (weltweite) Verbindung von Netzwerken
- gemeinsame Sprache: Internet Protocol (IP)
- darauf aufsetzende Protokolle, z.B. SMTP, HTTP ...

Das Internet

Ein Netzwerk aus Computer-Netzwerken

- Netzwerk: Verbindung von Computern
- $\Rightarrow$ Internet: (weltweite) Verbindung von Netzwerken
- gemeinsame Sprache: Internet Protocol (IP)
- darauf aufsetzende Protokolle, z.B. SMTP, HTTP ...

Offenheit und Flexiblität

Das Internet

Ein Netzwerk aus Computer-Netzwerken

- Netzwerk: Verbindung von Computern
- $\Rightarrow$ Internet: (weltweite) Verbindung von Netzwerken
- gemeinsame Sprache: Internet Protocol (IP)
- darauf aufsetzende Protokolle, z.B. SMTP, HTTP ...

Offenheit und Flexiblität

- einfacher Transport: Router müssen nur IP können

Das Internet

Ein Netzwerk aus Computer-Netzwerken

- Netzwerk: Verbindung von Computern
- $\Rightarrow$ Internet: (weltweite) Verbindung von Netzwerken
- gemeinsame Sprache: Internet Protocol (IP)
- darauf aufsetzende Protokolle, z.B. SMTP, HTTP ...

Offenheit und Flexiblität

- einfacher Transport: Router müssen nur IP können
- unabhängig vom Inhalt

Das Internet

Ein Netzwerk aus Computer-Netzwerken

- Netzwerk: Verbindung von Computern
- $\Rightarrow$ Internet: (weltweite) Verbindung von Netzwerken
- gemeinsame Sprache: Internet Protocol (IP)
- darauf aufsetzende Protokolle, z.B. SMTP, HTTP ...

Offenheit und Flexiblität

- einfacher Transport: Router müssen nur IP können
- unabhängig vom Inhalt
- Innovation einfach

Das Internet

Ein Netzwerk aus Computer-Netzwerken

- Netzwerk: Verbindung von Computern
- $\Rightarrow$ Internet: (weltweite) Verbindung von Netzwerken
- gemeinsame Sprache: Internet Protocol (IP)
- darauf aufsetzende Protokolle, z.B. SMTP, HTTP ...

Offenheit und Flexiblität

- einfacher Transport: Router müssen nur IP können
- unabhängig vom Inhalt
- Innovation einfach
- schnell

Das Internet

Ein Netzwerk aus Computer-Netzwerken

- Netzwerk: Verbindung von Computern
- $\Rightarrow$ Internet: (weltweite) Verbindung von Netzwerken
- gemeinsame Sprache: Internet Protocol (IP)
- darauf aufsetzende Protokolle, z.B. SMTP, HTTP ...

Offenheit und Flexiblität

- einfacher Transport: Router müssen nur IP können
- unabhängig vom Inhalt
- Innovation einfach
- schnell
- Gleichbehandlung

Inhaltsverzeichnis

Die IP-Adresse

Eine digitale Adresse

Die IP-Adresse

Eine digitale Adresse

- Internet Protocol (IP)

Die IP-Adresse

Eine digitale Adresse

- Internet Protocol (IP)
- jedes Gerät (global) eindeutige Adresse

Die IP-Adresse

Eine digitale Adresse

- Internet Protocol (IP)
- jedes Gerät (global) eindeutige Adresse
- Ausnahmen: Privater Adressraum sowie NAT

Die IP-Adresse

Eine digitale Adresse

- Internet Protocol (IP)
- jedes Gerät (global) eindeutige Adresse
- Ausnahmen: Privater Adressraum sowie NAT
- Nachverfolgung zu Geräten systemimmanent,

Die IP-Adresse

Eine digitale Adresse

- Internet Protocol (IP)
- jedes Gerät (global) eindeutige Adresse
- Ausnahmen: Privater Adressraum sowie NAT
- Nachverfolgung zu Geräten systemimmanent,
- Identifizierung von Personen schwer

Die IP-Adresse

Eine digitale Adresse

- Internet Protocol (IP)
- jedes Gerät (global) eindeutige Adresse
- Ausnahmen: Privater Adressraum sowie NAT
- Nachverfolgung zu Geräten systemimmanent,
- Identifizierung von Personen schwer

Beispiel

172.16.254.1

Inhaltsverzeichnis

Das Telefonbuch des Internets

Das Domain Name System

Das Telefonbuch des Internets

Das Domain Name System

- Namen sind einfacher zu merken als IP-Adressen

Das Telefonbuch des Internets

Das Domain Name System

- Namen sind einfacher zu merken als IP-Adressen
- Adressen können sich ändern

Das Telefonbuch des Internets

Das Domain Name System

- Namen sind einfacher zu merken als IP-Adressen
- Adressen können sich ändern
- $\Rightarrow$ DNS: Eine Art Telefonbuch

Das Telefonbuch des Internets

Das Domain Name System

- Namen sind einfacher zu merken als IP-Adressen
- Adressen können sich ändern
- $\Rightarrow$ DNS: Eine Art Telefonbuch
- hierarchisch

Das Telefonbuch des Internets

Das Domain Name System

- Namen sind einfacher zu merken als IP-Adressen
- Adressen können sich ändern
- $\Rightarrow$ DNS: Eine Art Telefonbuch
- hierarchisch
- unsichtbar, meist vom ISP, Alternativen möglich

Das Telefonbuch des Internets

Das Domain Name System

- Namen sind einfacher zu merken als IP-Adressen
- Adressen können sich ändern
- $\Rightarrow$ DNS: Eine Art Telefonbuch
- hierarchisch
- unsichtbar, meist vom ISP, Alternativen möglich

Beispiel

subdomain.domain.tld

Inhaltsverzeichnis

Das World Wide Web (WWW)

Verlinkte Information

Das World Wide Web (WWW)

Verlinkte Information

- HyperText Transfer Protokol (HTTP)

Das World Wide Web (WWW)

Verlinkte Information

- HyperText Transfer Protokol (HTTP)
- Homepages in Formatierungssprache HTML (HyperText Markup Language)

Das World Wide Web (WWW)

Verlinkte Information

- HyperText Transfer Protokol (HTTP)
- Homepages in Formatierungssprache HTML (HyperText Markup Language)
- offene (gemeinsame) Entwicklung

Das World Wide Web (WWW)

Verlinkte Information

- HyperText Transfer Protokol (HTTP)
- Homepages in Formatierungssprache HTML (HyperText Markup Language)
- offene (gemeinsame) Entwicklung
- Standardisierung (W3C)

Das World Wide Web (WWW)

Verlinkte Information

- HyperText Transfer Protokol (HTTP)
- Homepages in Formatierungssprache HTML (HyperText Markup Language)
- offene (gemeinsame) Entwicklung
- Standardisierung (W3C)

Standards

Das World Wide Web (WWW)

Verlinkte Information

- HyperText Transfer Protokol (HTTP)
- Homepages in Formatierungssprache HTML (HyperText Markup Language)
- offene (gemeinsame) Entwicklung
- Standardisierung (W3C)

Standards

- richtige Umsetzung wichtig!!!!!!!!

Das World Wide Web (WWW)

Verlinkte Information

- HyperText Transfer Protokol (HTTP)
- Homepages in Formatierungssprache HTML (HyperText Markup Language)
- offene (gemeinsame) Entwicklung
- Standardisierung (W3C)

Standards

- richtige Umsetzung wichtig!!!!!!!!
- z.B. Zugang für Sehbehinderte

Das World Wide Web (WWW)

Verlinkte Information

- HyperText Transfer Protokol (HTTP)
- Homepages in Formatierungssprache HTML (HyperText Markup Language)
- offene (gemeinsame) Entwicklung
- Standardisierung (W3C)

Standards

- richtige Umsetzung wichtig!!!!!!!!
- z.B. Zugang für Sehbehinderte
- Maschinenlesbarkeit, z.B. für News-Feeds

Webserver

- Webserver = Computer

Webserver

- Webserver = Computer
- hat IP-Adresse und Domainnamen

Webserver

- Webserver = Computer
- hat IP-Adresse und Domainnamen
- kann mehrere Domainnamen haben, viele Homepages anbieten (Shared-Hosting)

Webserver

- Webserver = Computer
- hat IP-Adresse und Domainnamen
- kann mehrere Domainnamen haben, viele Homepages anbieten (Shared-Hosting)

HTTPS

Webserver

- Webserver = Computer
- hat IP-Adresse und Domainnamen
- kann mehrere Domainnamen haben, viele Homepages anbieten (Shared-Hosting)

HTTPS

- Jeder auf dem Übertragungsweg kann mitlesen (Rechenzentrum bis W-Lan Zuhause)

Webserver

- Webserver = Computer
- hat IP-Adresse und Domainnamen
- kann mehrere Domainnamen haben, viele Homepages anbieten (Shared-Hosting)

HTTPS

- Jeder auf dem Übertragungsweg kann mitlesen (Rechenzentrum bis W-Lan Zuhause)
- daher: HTTPS Verschlüsselung

Webserver

- Webserver = Computer
- hat IP-Adresse und Domainnamen
- kann mehrere Domainnamen haben, viele Homepages anbieten (Shared-Hosting)

HTTPS

- Jeder auf dem Übertragungsweg kann mitlesen (Rechenzentrum bis W-Lan Zuhause)
- daher: HTTPS Verschlüsselung
- vertrauenswürdige(?) Zertifizierungsstellen

Webserver

- Webserver = Computer
- hat IP-Adresse und Domainnamen
- kann mehrere Domainnamen haben, viele Homepages anbieten (Shared-Hosting)

HTTPS

- Jeder auf dem Übertragungsweg kann mitlesen (Rechenzentrum bis W-Lan Zuhause)
- daher: HTTPS Verschlüsselung
- vertrauenswürdige(?) Zertifizierungsstellen
- Benutzen!!!!!!!

Inhaltsverzeichnis

E-Mail und Sicherheit

Post in der digitalen Gesellschaft

E-Mail und Sicherheit

Post in der digitalen Gesellschaft

- SMTP

E-Mail und Sicherheit

Post in der digitalen Gesellschaft

- SMTP
- Store and Forward

E-Mail und Sicherheit

Post in der digitalen Gesellschaft

- SMTP
- Store and Forward
- bleibt beim Zielserver oder Mailprogramm gespeichert

E-Mail und Sicherheit

Post in der digitalen Gesellschaft

- SMTP
- Store and Forward
- bleibt beim Zielserver oder Mailprogramm gespeichert
- ungefähr so sicher wie Postkarte: Jeder kann Absender fälschen und jeder auf dem Transportweg mitlesen/speichern/verändern

E-Mail und Sicherheit

Post in der digitalen Gesellschaft

- SMTP
- Store and Forward
- bleibt beim Zielserver oder Mailprogramm gespeichert
- ungefähr so sicher wie Postkarte: Jeder kann Absender fälschen und jeder auf dem Transportweg mitlesen/speichern/verändern

Sichere Kommunikation

E-Mail und Sicherheit

Post in der digitalen Gesellschaft

- SMTP
- Store and Forward
- bleibt beim Zielserver oder Mailprogramm gespeichert
- ungefähr so sicher wie Postkarte: Jeder kann Absender fälschen und jeder auf dem Transportweg mitlesen/speichern/verändern

Sichere Kommunikation

- Verschlüsselung

E-Mail und Sicherheit

Post in der digitalen Gesellschaft

- SMTP
- Store and Forward
- bleibt beim Zielserver oder Mailprogramm gespeichert
- ungefähr so sicher wie Postkarte: Jeder kann Absender fälschen und jeder auf dem Transportweg mitlesen/speichern/verändern

Sichere Kommunikation

- Verschlüsselung
- Signaturen / Verifikation

E-Mail und Sicherheit

Post in der digitalen Gesellschaft

- SMTP
- Store and Forward
- bleibt beim Zielserver oder Mailprogramm gespeichert
- ungefähr so sicher wie Postkarte: Jeder kann Absender fälschen und jeder auf dem Transportweg mitlesen/speichern/verändern

Sichere Kommunikation

- Verschlüsselung
- Signaturen / Verifikation
- Benutzen!!!!!!!

E-Mail und Sicherheit

Post in der digitalen Gesellschaft

- SMTP
- Store and Forward
- bleibt beim Zielserver oder Mailprogramm gespeichert
- ungefähr so sicher wie Postkarte: Jeder kann Absender fälschen und jeder auf dem Transportweg mitlesen/speichern/verändern

Sichere Kommunikation

- Verschlüsselung
- Signaturen / Verifikation
- Benutzen!!!!!!!
- Metadaten kaum zu verhindern

Inhaltsverzeichnis

Verschlüsselung

Privatsphäre im öffentlichen Netz

Verschlüsselung

Privatsphäre im öffentlichen Netz

- Vertraulichkeit herstellen?

Verschlüsselung

Privatsphäre im öffentlichen Netz

- Vertraulichkeit herstellen?
- könnte abgefangen, gelesen, gespeichert, verändert werden

Verschlüsselung

Privatsphäre im öffentlichen Netz

- Vertraulichkeit herstellen?
- könnte abgefangen, gelesen, gespeichert, verändert werden
- ohne dass jemand es mitbekommt

Verschlüsselung

Privatsphäre im öffentlichen Netz

- Vertraulichkeit herstellen?
- könnte abgefangen, gelesen, gespeichert, verändert werden
- ohne dass jemand es mitbekommt
- $\Rightarrow$ Verschlüsselung

Kryptografie

- rasante Entwicklung folgte der Computertechnologie

Kryptografie

- rasante Entwicklung folgte der Computertechnologie
- Heute: Einfache und schnelle Anwendung

Kryptografie

- rasante Entwicklung folgte der Computertechnologie
- Heute: Einfache und schnelle Anwendung
- sehr schnelles(*) Knacken einfacher(*) Verfahren

Kryptografie

- rasante Entwicklung folgte der Computertechnologie
- Heute: Einfache und schnelle Anwendung
- sehr schnelles(*) Knacken einfacher(*) Verfahren
- **kein Allheilmittel, keine vollkommene Sicherheit**

Kryptografie

- rasante Entwicklung folgte der Computertechnologie
- Heute: Einfache und schnelle Anwendung
- sehr schnelles(*) Knacken einfacher(*) Verfahren
- **kein Allheilmittel, keine vollkommene Sicherheit**
- muss richtig angewendet werden

Kryptografie

- rasante Entwicklung folgte der Computertechnologie
- Heute: Einfache und schnelle Anwendung
- sehr schnelles(*) Knacken einfacher(*) Verfahren
- **kein Allheilmittel, keine vollkommene Sicherheit**
- muss richtig angewendet werden
- mathematisch Sicherheit nachweisbar(?)

Kryptografie

- rasante Entwicklung folgte der Computertechnologie
- Heute: Einfache und schnelle Anwendung
- sehr schnelles(*) Knacken einfacher(*) Verfahren
- **kein Allheilmittel, keine vollkommene Sicherheit**
- muss richtig angewendet werden
- mathematisch Sicherheit nachweisbar(?)
- Verfahren: symmetrisch und assymmetrisch

Kryptografie

- rasante Entwicklung folgte der Computertechnologie
- Heute: Einfache und schnelle Anwendung
- sehr schnelles(*) Knacken einfacher(*) Verfahren
- **kein Allheilmittel, keine vollkommene Sicherheit**
- muss richtig angewendet werden
- mathematisch Sicherheit nachweisbar(?)
- Verfahren: symmetrisch und assymmetrisch

mögliche Angriffe

Kryptografie

- rasante Entwicklung folgte der Computertechnologie
- Heute: Einfache und schnelle Anwendung
- sehr schnelles(*) Knacken einfacher(*) Verfahren
- **kein Allheilmittel, keine vollkommene Sicherheit**
- muss richtig angewendet werden
- mathematisch Sicherheit nachweisbar(?)
- Verfahren: symmetrisch und assymmetrisch

mögliche Angriffe

- vor/hinter der Verschlüsselung

Kryptografie

- rasante Entwicklung folgte der Computertechnologie
- Heute: Einfache und schnelle Anwendung
- sehr schnelles(*) Knacken einfacher(*) Verfahren
- **kein Allheilmittel, keine vollkommene Sicherheit**
- muss richtig angewendet werden
- mathematisch Sicherheit nachweisbar(?)
- Verfahren: symmetrisch und assymmetrisch

mögliche Angriffe

- vor/hinter der Verschlüsselung
- z.B. Trojaner/Keylogger auf dem Rechner

Kryptografie

- rasante Entwicklung folgte der Computertechnologie
- Heute: Einfache und schnelle Anwendung
- sehr schnelles(*) Knacken einfacher(*) Verfahren
- **kein Allheilmittel, keine vollkommene Sicherheit**
- muss richtig angewendet werden
- mathematisch Sicherheit nachweisbar(?)
- Verfahren: symmetrisch und assymmetrisch

mögliche Angriffe

- vor/hinter der Verschlüsselung
- z.B. Trojaner/Keylogger auf dem Rechner
- z.B. auf dem Server abfangen

Kryptografie

- rasante Entwicklung folgte der Computertechnologie
- Heute: Einfache und schnelle Anwendung
- sehr schnelles(*) Knacken einfacher(*) Verfahren
- **kein Allheilmittel, keine vollkommene Sicherheit**
- muss richtig angewendet werden
- mathematisch Sicherheit nachweisbar(?)
- Verfahren: symmetrisch und assymmetrisch

mögliche Angriffe

- vor/hinter der Verschlüsselung
- z.B. Trojaner/Keylogger auf dem Rechner
- z.B. auf dem Server abfangen
- geheimen Schlüssel besorgen

Kryptografie

- rasante Entwicklung folgte der Computertechnologie
- Heute: Einfache und schnelle Anwendung
- sehr schnelles(*) Knacken einfacher(*) Verfahren
- **kein Allheilmittel, keine vollkommene Sicherheit**
- muss richtig angewendet werden
- mathematisch Sicherheit nachweisbar(?)
- Verfahren: symmetrisch und assymmetrisch

mögliche Angriffe

- vor/hinter der Verschlüsselung
- z.B. Trojaner/Keylogger auf dem Rechner
- z.B. auf dem Server abfangen
- geheimen Schlüssel besorgen
- Metadaten

Inhaltsverzeichnis

Deep-Packet-Inspection

Werfen wir einen Blick in ihren Internetverkehr

Deep-Packet-Inspection

Werfen wir einen Blick in ihren Internetverkehr

- Bisher: nur Paket-Header auslesen, an Empfänger zustellen

Deep-Packet-Inspection

Werfen wir einen Blick in ihren Internetverkehr

- Bisher: nur Paket-Header auslesen, an Empfänger zustellen
- DPI: auch Inhalt anschauen

Deep-Packet-Inspection

Werfen wir einen Blick in ihren Internetverkehr

- Bisher: nur Paket-Header auslesen, an Empfänger zustellen
- DPI: auch Inhalt anschauen
- beides kann eine Firewall

Deep-Packet-Inspection

Werfen wir einen Blick in ihren Internetverkehr

- Bisher: nur Paket-Header auslesen, an Empfänger zustellen
- DPI: auch Inhalt anschauen
- beides kann eine Firewall
- unerwünschte Pakete aussperren (Hacking)

Deep-Packet-Inspection

Werfen wir einen Blick in ihren Internetverkehr

- Bisher: nur Paket-Header auslesen, an Empfänger zustellen
- DPI: auch Inhalt anschauen
- beides kann eine Firewall
- unerwünschte Pakete aussperren (Hacking)
- aber auch Inhalte überwachen, Werbung einblenden

Deep-Packet-Inspection

Werfen wir einen Blick in ihren Internetverkehr

- Bisher: nur Paket-Header auslesen, an Empfänger zustellen
- DPI: auch Inhalt anschauen
- beides kann eine Firewall
- unerwünschte Pakete aussperren (Hacking)
- aber auch Inhalte überwachen, Werbung einblenden
- siehe China

Deep-Packet-Inspection

Werfen wir einen Blick in ihren Internetverkehr

- Bisher: nur Paket-Header auslesen, an Empfänger zustellen
- DPI: auch Inhalt anschauen
- beides kann eine Firewall
- unerwünschte Pakete aussperren (Hacking)
- aber auch Inhalte überwachen, Werbung einblenden
- siehe China
- $\Rightarrow$ Verschlüsselung

Inhaltsverzeichnis

Peer-to-Peer

Von mir zu ihnen ohne jemanden dazwischen

Peer-to-Peer

Von mir zu ihnen ohne jemanden dazwischen

- Bisher: Zentralisiert, Alle Clients mit (einem) Server

Peer-to-Peer

Von mir zu ihnen ohne jemanden dazwischen

- Bisher: Zentralisiert, Alle Clients mit (einem) Server
- P2P: Teilnehmer (Peers) sind gleichberechtigt und reden direkt untereinander

Peer-to-Peer

Von mir zu ihnen ohne jemanden dazwischen

- Bisher: Zentralisiert, Alle Clients mit (einem) Server
- P2P: Teilnehmer (Peers) sind gleichberechtigt und reden direkt untereinander
- Vorteil: kein Single-Point-of-Failure, Teilnehmer steuern Ressourcen bei.

Peer-to-Peer

Von mir zu ihnen ohne jemanden dazwischen

- Bisher: Zentralisiert, Alle Clients mit (einem) Server
- P2P: Teilnehmer (Peers) sind gleichberechtigt und reden direkt untereinander
- Vorteil: kein Single-Point-of-Failure, Teilnehmer steuern Ressourcen bei.
- Nachteil: Hierarchisch ist einfacher

Peer-to-Peer

Von mir zu ihnen ohne jemanden dazwischen

- Bisher: Zentralisiert, Alle Clients mit (einem) Server
- P2P: Teilnehmer (Peers) sind gleichberechtigt und reden direkt untereinander
- Vorteil: kein Single-Point-of-Failure, Teilnehmer steuern Ressourcen bei.
- Nachteil: Hierarchisch ist einfacher
- Freiheit?

Peer-to-Peer

Von mir zu ihnen ohne jemanden dazwischen

- Bisher: Zentralisiert, Alle Clients mit (einem) Server
- P2P: Teilnehmer (Peers) sind gleichberechtigt und reden direkt untereinander
- Vorteil: kein Single-Point-of-Failure, Teilnehmer steuern Ressourcen bei.
- Nachteil: Hierarchisch ist einfacher
- Freiheit?
- wird benutzt für Videotelefonie, Filesharing, ...

Inhaltsverzeichnis

Verhaltensbasierte Werbung

Jetzt wird es persönlich

Verhaltensbasierte Werbung

Jetzt wird es persönlich

- Aktivitäten von Internetnutzern aufzeichnen

Verhaltensbasierte Werbung

Jetzt wird es persönlich

- Aktivitäten von Internetnutzern aufzeichnen
- Profile erstellen

Verhaltensbasierte Werbung

Jetzt wird es persönlich

- Aktivitäten von Internetnutzern aufzeichnen
- Profile erstellen
- effizientere (zugeschnittene) Werbung

Verhaltensbasierte Werbung

Jetzt wird es persönlich

- Aktivitäten von Internetnutzern aufzeichnen
- Profile erstellen
- effizientere (zugeschnittene) Werbung
- Tracking z.B. durch ID in Cookies (im Browser)

Verhaltensbasierte Werbung

Jetzt wird es persönlich

- Aktivitäten von Internetnutzern aufzeichnen
- Profile erstellen
- effizientere (zugeschnittene) Werbung
- Tracking z.B. durch ID in Cookies (im Browser)

Beispiel

Verhaltensbasierte Werbung

Jetzt wird es persönlich

- Aktivitäten von Internetnutzern aufzeichnen
- Profile erstellen
- effizientere (zugeschnittene) Werbung
- Tracking z.B. durch ID in Cookies (im Browser)

Beispiel

- Besucht eine Seite z.B. Fußball $\rightarrow$ Cookie wird erzeugt

Verhaltensbasierte Werbung

Jetzt wird es persönlich

- Aktivitäten von Internetnutzern aufzeichnen
- Profile erstellen
- effizientere (zugeschnittene) Werbung
- Tracking z.B. durch ID in Cookies (im Browser)

Beispiel

- Besucht eine Seite z.B. Fußball $\rightarrow$ Cookie wird erzeugt
- Besucht eine Seite über Autos $\rightarrow$ Cookie wird wiedererkannt

Verhaltensbasierte Werbung

Jetzt wird es persönlich

- Aktivitäten von Internetnutzern aufzeichnen
- Profile erstellen
- effizientere (zugeschnittene) Werbung
- Tracking z.B. durch ID in Cookies (im Browser)

Beispiel

- Besucht eine Seite z.B. Fußball $\rightarrow$ Cookie wird erzeugt
- Besucht eine Seite über Autos $\rightarrow$ Cookie wird wiedererkannt
- Verhaltensmarketingfirma speichert das

Verhaltensbasierte Werbung

Jetzt wird es persönlich

- Aktivitäten von Internetnutzern aufzeichnen
- Profile erstellen
- effizientere (zugeschnittene) Werbung
- Tracking z.B. durch ID in Cookies (im Browser)

Beispiel

- Besucht eine Seite z.B. Fußball $\rightarrow$ Cookie wird erzeugt
- Besucht eine Seite über Autos $\rightarrow$ Cookie wird wiedererkannt
- Verhaltensmarketingfirma speichert das
- vergleicht mit Profilen von ähnlichen Leuten, die sich für ähnliche Dinge interessieren

Verhaltensbasierte Werbung

Jetzt wird es persönlich

- Aktivitäten von Internetnutzern aufzeichnen
- Profile erstellen
- effizientere (zugeschnittene) Werbung
- Tracking z.B. durch ID in Cookies (im Browser)

Beispiel

- Besucht eine Seite z.B. Fußball $\rightarrow$ Cookie wird erzeugt
- Besucht eine Seite über Autos $\rightarrow$ Cookie wird wiedererkannt
- Verhaltensmarketingfirma speichert das
- vergleicht mit Profilen von ähnlichen Leuten, die sich für ähnliche Dinge interessieren
- $\rightarrow$ Bierwerbung

Probleme verhaltensbasierter Werbung

- Profiling für Strafverfolgung, Geheimdienste funktioniert genauso

Probleme verhaltensbasierter Werbung

- Profiling für Strafverfolgung, Geheimdienste funktioniert genauso
- Anonymisierte Daten zu Individuen rückverfolgbar?

Probleme verhaltensbasierter Werbung

- Profiling für Strafverfolgung, Geheimdienste funktioniert genauso
- Anonymisierte Daten zu Individuen rückverfolgbar?
- viele Daten sammeln $\Rightarrow$ sehr detaillierte Profile

Probleme verhaltensbasierter Werbung

- Profiling für Strafverfolgung, Geheimdienste funktioniert genauso
- Anonymisierte Daten zu Individuen rückverfolgbar?
- viele Daten sammeln $\Rightarrow$ sehr detaillierte Profile
- große Datenmengen verarbeitbar

Probleme verhaltensbasierter Werbung

- Profiling für Strafverfolgung, Geheimdienste funktioniert genauso
- Anonymisierte Daten zu Individuen rückverfolgbar?
- viele Daten sammeln $\Rightarrow$ sehr detaillierte Profile
- große Datenmengen verarbeitbar
- Google/Facebook/Amazon. Nebenerwerb von vielen Firmen

Probleme verhaltensbasierter Werbung

- Profiling für Strafverfolgung, Geheimdienste funktioniert genauso
- Anonymisierte Daten zu Individuen rückverfolgbar?
- viele Daten sammeln $\Rightarrow$ sehr detaillierte Profile
- große Datenmengen verarbeitbar
- Google/Facebook/Amazon. Nebenerwerb von vielen Firmen
- Opt-Out

Inhaltsverzeichnis

Die Suchmaschine

Ein Index für das Internet

Die Suchmaschine

Ein Index für das Internet

- Internet: (Hyper-)Links, alles verlinkbar, kein zentraler Index

Die Suchmaschine

Ein Index für das Internet

- Internet: (Hyper-)Links, alles verlinkbar, kein zentraler Index
- Suchmaschinen aka. Google

Die Suchmaschine

Ein Index für das Internet

- Internet: (Hyper-)Links, alles verlinkbar, kein zentraler Index
- Suchmaschinen aka. Google
- Crawler/Spider erstellen Index

Die Suchmaschine

Ein Index für das Internet

- Internet: (Hyper-)Links, alles verlinkbar, kein zentraler Index
- Suchmaschinen aka. Google
- Crawler/Spider erstellen Index
- sehr komplex

Die Suchmaschine

Ein Index für das Internet

- Internet: (Hyper-)Links, alles verlinkbar, kein zentraler Index
- Suchmaschinen aka. Google
- Crawler/Spider erstellen Index
- sehr komplex
- Pagerank / SEO ?

Die Suchmaschine

Ein Index für das Internet

- Internet: (Hyper-)Links, alles verlinkbar, kein zentraler Index
- Suchmaschinen aka. Google
- Crawler/Spider erstellen Index
- sehr komplex
- Pagerank / SEO ?
- Kommerzialisierung über Werbeeinblendungen

Inhaltsverzeichnis

Cloud Computing

Das Internet wird ihr Computer

Cloud Computing

Das Internet wird ihr Computer

- Werbeslogan

Cloud Computing

Das Internet wird ihr Computer

- Werbeslogan
- alles was irgendwo im Netzwerk abläuft und nicht auf dem eigenen Computer

Cloud Computing

Das Internet wird ihr Computer

- Werbeslogan
- alles was irgendwo im Netzwerk abläuft und nicht auf dem eigenen Computer
- von jedem Gerät aus abrufbar

Inhaltsverzeichnis

Social Media

Wo wir uns treffen

Social Media

Wo wir uns treffen

- Austausch nutzergenerierter Inhalte

Social Media

Wo wir uns treffen

- Austausch nutzergenerierter Inhalte
- interaktiv

Social Media

Wo wir uns treffen

- Austausch nutzergenerierter Inhalte
- interaktiv
- große Nutzerzahlen u großer Einfluss

Social Media

Wo wir uns treffen

- Austausch nutzergenerierter Inhalte
- interaktiv
- große Nutzerzahlen u großer Einfluss
- Bsp: Wikipedia, Blogs, YouTube/Flickr, Facebook/Google+, WoW

Social Media

Wo wir uns treffen

- Austausch nutzergenerierter Inhalte
- interaktiv
- große Nutzerzahlen u großer Einfluss
- Bsp: Wikipedia, Blogs, YouTube/Flickr, Facebook/Google+, WoW
- Probleme: Schutz der Privatsphäre, Datenschutz, Jugendschutz

Inhaltsverzeichnis

Digitale Demokratie

Internet Governance

Digitale Demokratie

Internet Governance

- Internet Governance

Digitale Demokratie

Internet Governance

- Internet Governance
- faszinierende Möglichkeiten

Digitale Demokratie

Internet Governance

- Internet Governance
- faszinierende Möglichkeiten
- Kollaboration (siehe: Wikipedia)

Digitale Demokratie

Internet Governance

- Internet Governance
- faszinierende Möglichkeiten
- Kollaboration (siehe: Wikipedia)
- Gemeinschaftsprojekte (siehe: Debian)

Digitale Demokratie

Internet Governance

- Internet Governance
- faszinierende Möglichkeiten
- Kollaboration (siehe: Wikipedia)
- Gemeinschaftsprojekte (siehe: Debian)
- Abstimmungen?

Digitale Demokratie

Internet Governance

- Internet Governance
- faszinierende Möglichkeiten
- Kollaboration (siehe: Wikipedia)
- Gemeinschaftsprojekte (siehe: Debian)
- Abstimmungen?
- (alle) Informationen für jeden auf Knopfdruck

Digitale Demokratie

Internet Governance

- Internet Governance
- faszinierende Möglichkeiten
- Kollaboration (siehe: Wikipedia)
- Gemeinschaftsprojekte (siehe: Debian)
- Abstimmungen?
- (alle) Informationen für jeden auf Knopfdruck
- globale Kommunikation

Inhaltsverzeichnis

Creative Commons

Mehr Nutzungsfreiheiten trotz Urheberrecht

Creative Commons

Mehr Nutzungsfreiheiten trotz Urheberrecht

- Dieser Teil des Vortrags basiert auf:
  WIE DAS INTERNET FUNKTIONIERT – Eine Anleitung für Entscheidungsträger und Interessierte
  `https://digitalegesellschaft.de/wp-content/uploads/2012/04/digiges_wie_das_internet_funktioniert.pdf`

Creative Commons

Mehr Nutzungsfreiheiten trotz Urheberrecht

- Dieser Teil des Vortrags basiert auf:
  WIE DAS INTERNET FUNKTIONIERT – Eine Anleitung für Entscheidungsträger und Interessierte
  `https://digitalegesellschaft.de/wp-content/uploads/2012/04/digiges_wie_das_internet_funktioniert.pdf`
- Lizenz: Creative Commons BY-SA 3.0 (Namensnennung, Weitergabe unter gleichen Bedingungen)

Creative Commons

Mehr Nutzungsfreiheiten trotz Urheberrecht

- Dieser Teil des Vortrags basiert auf:
  WIE DAS INTERNET FUNKTIONIERT – Eine Anleitung für Entscheidungsträger und Interessierte
  `https://digitalegesellschaft.de/wp-content/uploads/2012/04/digiges_wie_das_internet_funktioniert.pdf`
- Lizenz: Creative Commons BY-SA 3.0 (Namensnennung, Weitergabe unter gleichen Bedingungen)
- Creative Commons ist eine Non-Profit Organisation

Creative Commons

Mehr Nutzungsfreiheiten trotz Urheberrecht

- Dieser Teil des Vortrags basiert auf:
  WIE DAS INTERNET FUNKTIONIERT – Eine Anleitung für Entscheidungsträger und Interessierte
  `https://digitalegesellschaft.de/wp-content/uploads/2012/04/digiges_wie_das_internet_funktioniert.pdf`
- Lizenz: Creative Commons BY-SA 3.0 (Namensnennung, Weitergabe unter gleichen Bedingungen)
- Creative Commons ist eine Non-Profit Organisation
- bietet verschiedene freie Lizenzverträge an (zum Zusammenklicken)

Creative Commons

Mehr Nutzungsfreiheiten trotz Urheberrecht

- Dieser Teil des Vortrags basiert auf:
  WIE DAS INTERNET FUNKTIONIERT – Eine Anleitung für Entscheidungsträger und Interessierte
  `https://digitalegesellschaft.de/wp-content/uploads/2012/04/digiges_wie_das_internet_funktioniert.pdf`
- Lizenz: Creative Commons BY-SA 3.0 (Namensnennung, Weitergabe unter gleichen Bedingungen)
- Creative Commons ist eine Non-Profit Organisation
- bietet verschiedene freie Lizenzverträge an (zum Zusammenklicken)
- bieten zusätzliche Freiheiten für kreative Werke

Creative Commons

Mehr Nutzungsfreiheiten trotz Urheberrecht

- Dieser Teil des Vortrags basiert auf:
  WIE DAS INTERNET FUNKTIONIERT – Eine Anleitung für Entscheidungsträger und Interessierte
  `https://digitalegesellschaft.de/wp-content/uploads/2012/04/digiges_wie_das_internet_funktioniert.pdf`
- Lizenz: Creative Commons BY-SA 3.0 (Namensnennung, Weitergabe unter gleichen Bedingungen)
- Creative Commons ist eine Non-Profit Organisation
- bietet verschiedene freie Lizenzverträge an (zum Zusammenklicken)
- bieten zusätzliche Freiheiten für kreative Werke
- `www.creativecommons.de`

Inhaltsverzeichnis

Fragen

?

Teaser: Teil X

Alles Compi - Teil X

Datenschutz und Privatsphäre

Hendrik Langer

emo-essen.de

??. Sep 2013

Inhaltsverzeichnis

Inhalte

- Wo und Wie Datenspuren anfallen (im Internet)
- Wer diese Daten haben will
- Wie diese Daten gesammelt werden
- Wie man verhindern kann, dass die eigenen Daten gesammelt werden

Inhaltsverzeichnis

So kurz wie möglich: Worauf sollte ich beim Surfen achten? I

- Lange und komplizierte Passwörter: Je länger, desto weniger wirr brauchen sie zu sein. Kürzer als 12, eher 14 Zeichen sollten sie auf keinen Fall sein. Generell sollten Sie Dinge wie Telefonnummern, Geburtstage, Namen des Haustiers oder ähnliche leicht zu ratenden Daten vermeiden. Denken Sie sich am besten einen Satz aus, nehmen Sie dessen Anfangsbuchstaben und streuen Sie noch etwas Zahlen und Interpunktionszeichen ein. Literaturzitate oder Liedanfänge sollten Sie dabei auch vermeiden. Wechseln Sie Ihre Passworte häufig. Verwenden Sie möglichst viele unterschiedliche Passwörter für Ihre verschiedenen Konten. Versuchen Sie, dabei nicht wahnsinnig zu werden.

So kurz wie möglich: Worauf sollte ich beim Surfen achten? II

- Überlegen Sie bei Webformularen, ob Sie wirklich alle abgefragten Daten einfüllen müssen. Rechtlich müssen Sie nur die Angaben nennen, welche die Gegenseite unbedingt zur Erfüllung der gewünschten Dienstleistung braucht. Fragt ein Formular penetrant nach Ihrer Telefonnummer, ohne dass Ihnen klar ist, wozu das gut sein soll, könnte Ihnen möglicherweise eine Fehleingabe unterlaufen. Wenn Sie Ihre Mailadresse angeben sollen, aber absehen können, dass Sie nicht lang mit der Gegenseite zu tun haben wollen, verwenden Sie Wegwerf-Mailadressen.
- Verschlüsseln Sie, so oft es geht. Versuchen Sie, ob sich Seiten statt mit http: nicht auch mit https: aufrufen lassen. Das Add-On „Https Everywhere“ unterstützt Sie hierbei.

So kurz wie möglich: Worauf sollte ich beim Surfen achten? III

- Halten Sie Ihren Rechner und die darauf installierte Software auf dem aktuellen Stand. Auf Betriebssystemseite sollte das automatisch gehen. Für die anderen Programme gibt es unter Windows Hilfswerkzeuge, welche das Aktuellhalten erleichtern.
- Verwenden Sie unter Windows einen Virenscanner und lassen Sie die lokale Firewall eingeschaltet.
- Installieren Sie nur Software aus vertrauenswürdigen Quellen. Die neueste MS-Office-Version von irgendeiner obskuren Warez-Site ist nicht nur illegal sondern auch mit einiger Wahrscheinlichkeit verseucht.
- Vorsicht beim Öffnen von Mailanhängen. Unerwartete Zustellbescheinigungen eines Paketlieferdienstes, angebliche Softwareupdates Ihrer Bank oder wirre Rechnungen, zu denen sich weitere Informationen im Anhang befinden sollen, haben normalerweise nur ein Ziel: Sie sollen verleitet werden, den Anhang auszuführen und damit Ihr System zu verseuchen.

So kurz wie möglich: Worauf sollte ich beim Surfen achten? IV

Inhaltsverzeichnis

Fragen

?

Teaser: Teil 2

Alles Compi - Teil 2

Installationsparty

Hendrik Langer

emo-essen.de

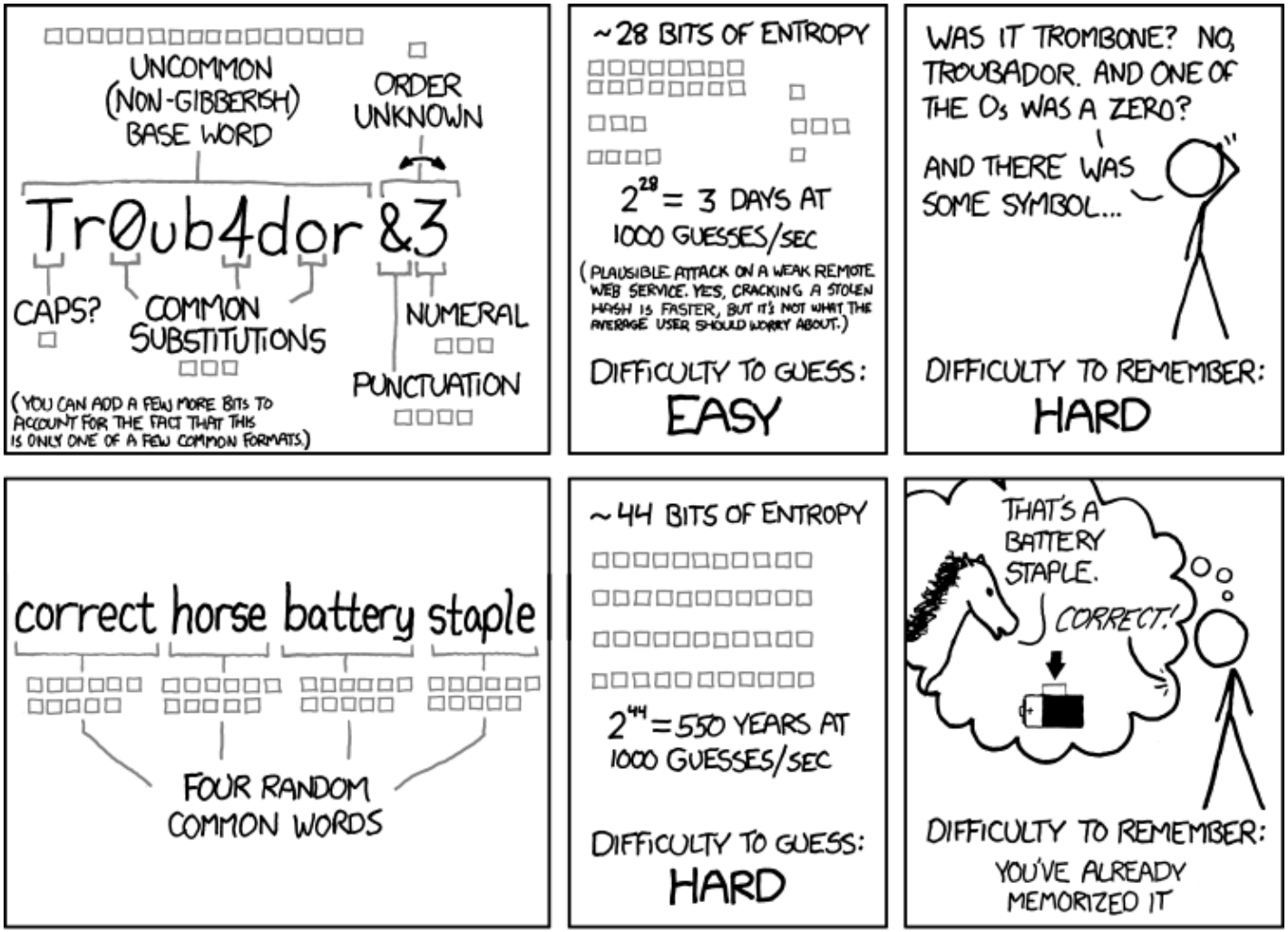
24. Sep 2013

Inhaltsverzeichnis

Inhalte

- Wie man seine E-Mails mit PGP oder S/MIME verschlüsselt und verschlüsselte Mails empfängt
  (besser noch: wie man gleich was besseres als E-Mail verwendet)
- Wie man seine Datenträger verschlüsselt
- Was ein gutes Passwort ist

Passwörter I



(CC-

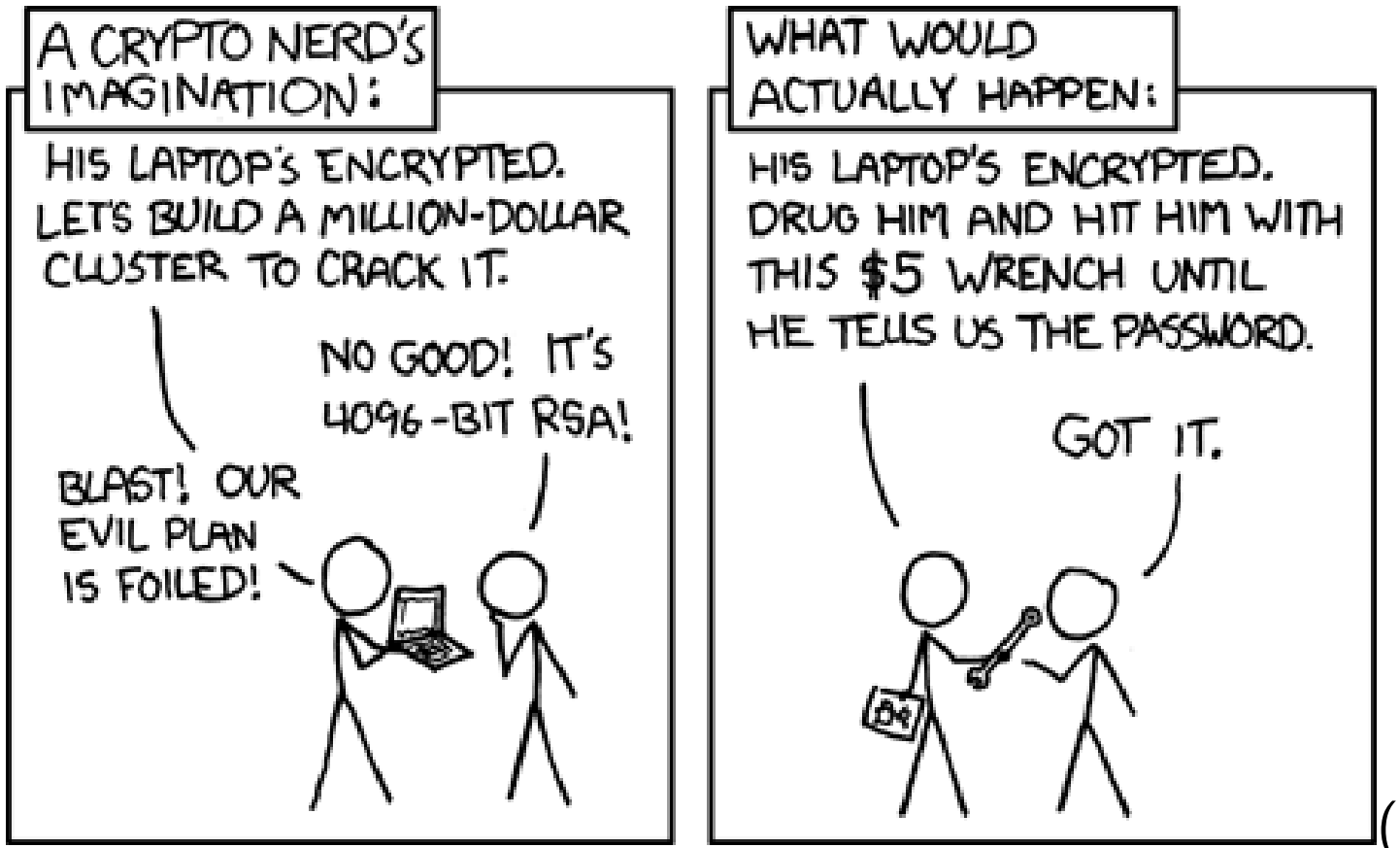
Passwörter II

BY-NC) Randall Munroe `http://xkcd.com/936/`

Passwörter III

- Password Reuse

Passwörter IV



- (CC-BY-NC) Randall Munroe `http://xkcd.com/538/`

Passwörter V

- https://en.wikipedia.org/wiki/Password_strength
- http://blog.zdf.de/hyperland/2010/11/ab_in_den_knast_fur_verschluss/

Inhaltsverzeichnis

Inhaltsverzeichnis

Verschlüsselung I

Verschlüsselung II

Die Teilnehmenden wissen/können nach der Party:

- Was asymmetrische Verschlüsselung ist und wie sie bei PGP und S/MIME zum Einsatz kommt
- was ein Diffie-Hellman Schlüsseltausch ist
- können und haben ein Schlüssel-Paar erstellt
- haben den öffentlichen Schlüssel an einen PGP Keyserver gesendet (oder lieber nicht, weil sie dort harvested werden)
- haben ihre Schlüssel-Informationen bestätigt
- Die Schlüssel-Informationen der anderen geprüft
- haben von jedem die Identität für die IDs, die sie signieren wollen, geprüft
- haben alle geprüften IDs auf den geprüften Schlüsseln signiert
- Die signierten Schlüssel an den gewählten PGP Keyserver oder an den Schlüssel-Besitzer zurückgeschickt
- machen einen Praxistest z.B. in deiner Gemeinde. (Sollte hier kein öffentlicher Schlüssel vorhanden sein, ist eine sofortige Beantragung dringend erforderlich.)

Inhaltsverzeichnis

Inhaltsverzeichnis

Inhaltsverzeichnis

Inhaltsverzeichnis

Inhaltsverzeichnis

Inhaltsverzeichnis

Fragen

?

Inhaltsverzeichnis

Fragen

?