Tag der Informatik-Lehrerinnen und -Lehrer 2015

Operations Security -
Sicherheit zwischen Script Kiddies und Geheimdiensten

München, 03. Juli 2015
Andreas Janning
https://www.openrightsgroup.org/

https://www.cse.umich.edu/
Internet Voting in Estonia

<table>
<thead>
<tr>
<th>Year</th>
<th>Percent of votes cast online</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local 2005</td>
<td>1</td>
</tr>
<tr>
<td>National 2007</td>
<td>4</td>
</tr>
<tr>
<td>European 2009</td>
<td>14</td>
</tr>
<tr>
<td>Local 2009</td>
<td>15</td>
</tr>
<tr>
<td>National 2011</td>
<td>25</td>
</tr>
<tr>
<td>Local 2013</td>
<td>20</td>
</tr>
<tr>
<td>European 2014</td>
<td>30</td>
</tr>
</tbody>
</table>
Was sind die Anforderungen an ein E-Voting System?

■ Integrität – Das Ergebnis entspricht dem Willen der Wähler
  ■ Die Stimmen werden so abgegeben wie es der Wähler wollte
  ■ Die Stimmen werden so gezählt wie sie abgegeben wurden
  ■ Jeder Wähler hat nur eine Stimme

■ Geheimhaltung – Das Wahlgeheimnis ist gewahrt
  ■ Niemand kann herausfinden für wen ich gestimmt hat
  ■ Selbst wenn ich versuche es jemandem zu beweisen
Estonia hit by 'Moscow cyber war'

Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.

Many of the attacks have come from Russia and are being hosted by Russian state computer servers, Tallinn says. Moscow denies any involvement.

Estonia says the attacks began after it moved a Soviet war memorial in Tallinn. The move was condemned by the Kremlin.

A Nato spokesman said the organisation was giving Estonia technical help.
Architecture Time!

- Voting-Server
- Counting-Server
- Client
- Verifier App
encryptedBallot = encryptRSA(publicKeyElection, vote + randomPad)

signedBallot = sign(secretKeyVoter, encryptedBallot)

send(TLSClientAuth, signedBallot)
Voting - Server

Client

Verifier App

signed encrypted Ballot

encrypt(publicKeyElection , Obama + knownPad)
encrypt(publicKeyElection , Romney + knownPad)
encrypt(publicKeyElection , Dr. Evil + knownPad)
Voting-Server \( \rightarrow \) signed encrypted Ballot \( \rightarrow \) Counting-Server

- DVD
- decrypt(SecretKeyElection, encryptedBallot)
- count(ballots)
Ist das System angreifbar?
Client Side

Client

Voting Server

steal pin

cast vote

Voting Server

cast new vote

Client

wait 30 minutes

infect client
Server-Side

Counting-Server

Buildserver

infect

applyBetterMath()
Operational Security

Our security is better than Google’s.

— Toomas Hendrik Ilves
President of Estonia
**Notepad2**

Current Release: Version 4.2.25  
Development Version: 5.0.26_beta4  
Project last updated: October 28, 2012

The Story so far...

A few years ago, I found myself writing my first PHP projects using *metapad*. When I was looking around for better text editors with syntax highlighting, I have come across the *Scintilla* source code editing component. I was very impressed by this project, so I decided to create my own Scintilla-based text editor.

The result is **Notepad2**, a fast and light-weight Notepad-like text editor with syntax highlighting. This program can be run out of the box without installation, and does not touch your system's registry.

**Downloads**

- Download Notepad2 4.2.25 Program Files (x86) [305 KB]
- Download Notepad2 4.2.25 Program Files (x64) [371 KB]
- Download Notepad2 4.2.25 Setup (x86) [292 KB]
- Download Notepad2 4.2.25 Setup (x64) [351 KB]
- Download Notepad2 4.2.25 Source Code [217 KB]
Haletamiseks peate enne tuntamist ID-kaardi või mobiil-ID abil:
“nice people who care about computer hygiene have no viruses”

“In practice, computer risks have been eliminated”

“They’re here not because of their technical savvy, but their politically suitable (although technically incompetent) message”
Aber betrifft uns das überhaupt?
Middle school student charged with cybercrime in Holiday

Green had previously received a three-day suspension for accessing the system inappropriately. Other students also got in trouble at the time, he said. It was a well-known trick, Green said, because the password was easy to remember: a teacher's last name. He said he discovered it by watching the teacher type it in.

The school district is in the process of changing the network password, district spokeswoman Linda Cobbe said.
Studie: Industriespionage 2014

Gab es in Ihrem Unternehmen konkrete Spionagefälle?

Deutschland

Nein 45,7 %
Ja 26,9 %
Verdacht 27,4 %

Quelle: Corporate Trust
Nach Hackerangriff: Bundestagsnetzwerk wird mehrere Tage komplett abgeschaltet

Von Sven Röbel und Maik Baumgartner

Bundestagspräsident Norbert Lammert: Schlechte Nachricht für die Abgeordneten

Nach dem Cyberangriff auf den Bundestag werden bald Teile des IT-Systems neu aufgesetzt. Für die Abgeordneten ist das ärgerlich: Sie müssen tagelang auf das Bundestagsnetzwerk verzichten.
Neue Dokumente von WikiLeaks

Großer NSA-Lauschangangriff auf Bundesregierung
<table>
<thead>
<tr>
<th>TOPI</th>
<th>Selector</th>
<th>Subscriber_ID</th>
<th>Information_Need</th>
<th>TOPI_Add_Date</th>
<th>Priority</th>
<th>IN_Explainer</th>
</tr>
</thead>
<tbody>
<tr>
<td>S2C32</td>
<td>+49228682XXXX</td>
<td>MOF ASCHEBRENNER</td>
<td>2002-388*</td>
<td>101215</td>
<td>2</td>
<td>Germany: Political Affairs</td>
</tr>
<tr>
<td>S2C32</td>
<td>+4922817XXXX</td>
<td>OFF 400 FOR ECON POLICY</td>
<td>2002-388*</td>
<td>101215</td>
<td>2</td>
<td>Germany: Political Affairs</td>
</tr>
<tr>
<td>S2C32</td>
<td>+4922817XXXX</td>
<td>OFF 400 FOR ECON POLICY</td>
<td>2002-388*</td>
<td>101215</td>
<td>2</td>
<td>Germany: Political Affairs</td>
</tr>
<tr>
<td>S2C32</td>
<td>+4922817XXXX</td>
<td>OFF 400 FOR ECON POLICY</td>
<td>2002-388*</td>
<td>101215</td>
<td>2</td>
<td>Germany: Political Affairs</td>
</tr>
<tr>
<td>S2C32</td>
<td>+49228682XXXX</td>
<td>BUNDESMINISTERIUM DER FINANZEN MONEY LOAN DEPT</td>
<td>2003-2777*</td>
<td>101215</td>
<td>2</td>
<td>Multi-country: International Finance Developments</td>
</tr>
<tr>
<td>S2C32</td>
<td>+49228682XXXX</td>
<td>GE INT BS FIN MIN CZAKERT</td>
<td>2003-2777*</td>
<td>101215</td>
<td>2</td>
<td>Multi-country: International Finance Developments</td>
</tr>
<tr>
<td>S2C32</td>
<td>+49691344XXXX</td>
<td>EUROPEAN CENTRAL BANK</td>
<td>2003-2777*</td>
<td>110111</td>
<td>3</td>
<td>Multi-country: International Finance Developments</td>
</tr>
<tr>
<td>S2C32</td>
<td>+49228682XXXX</td>
<td>GERMAN FIN MIN STATE SEC</td>
<td>2002-388*</td>
<td>101215</td>
<td>2</td>
<td>Germany: Political Affairs</td>
</tr>
<tr>
<td>S2C32</td>
<td>+49228682XXXX</td>
<td>GERMAN MINIST FINANCE</td>
<td>2002-388*</td>
<td>101215</td>
<td>2</td>
<td>Germany: Political Affairs</td>
</tr>
<tr>
<td>S2C32</td>
<td>+49228682XXXX</td>
<td>GE INT TR MIN OF FIN HEND</td>
<td>2002-388*</td>
<td>101215</td>
<td>2</td>
<td>Germany: Political Affairs</td>
</tr>
</tbody>
</table>
(TSI/SII/REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.
(TS//SI/NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

(TS//SI/NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon
(TS//SI//REL TO USA,FVEY) The CTX4000 is a portable continuous wave (CW) radar unit. It can be used to illuminate a target system to recover different off net information. Primary uses include VAGRANT and DROPMIRE collection.

---

(TS//SI//REL TO USA,FVEY) The CTX4000 provides the means to collect signals that otherwise would not be collectable, or would be extremely difficult to collect and process. It provides the following features:

- **Frequency Range:** 1 - 2 GHz.
- **Bandwidth:** Up to 45 MHz
- **Output Power:** User adjustable up to 2 W using the internal amplifier; external amplifiers make it possible to go up to 1 kW.
- **Phase adjustment with front panel knob**
What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works

1. Target
2. Internet Router
3. Yahoo’s Web Server
4. SSO Site
5. TAO FOXACID Server
6. NSA

5. FOXACID packet beats the Yahoo packet back to the endpoint
Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- Special Requests

Complete list and details on PRISM web page:
Go PRISMFAA
What can we do?

- Im WWW
  - mit HTTPS Everywhere TLS enforcen
  - https://www.eff.org/de/https-everywhere

- Mit TOR wirklich anonym surfen
  - https://www.torproject.org/
What can we do?

- In der Kommunikation
  - Emails verschlüsseln mit PGP
    - https://www.gnupg.org/
  - Mit OTR NSA-Sicher chatten
What can we do?

- Auf dem Handy verschlüsselt telefonieren und chatten
  - Auf Android mit Redphone und Textsecure
  - https://whispersystems.org/
- Auf Iphone mit Signal
  - https://whispersystems.org/
What can we do?

- Auf dem eigenen Rechner
  - Die Festplatte verschlüsseln mit Truecrypt
  - http://www.heise.de/download/truecrypt.html
- Und Passwörter mit Keepass
  - http://keepass.info/
What can we do?

- Oder das Gesamtpaket: TailsOS
- https://tails.boum.org/