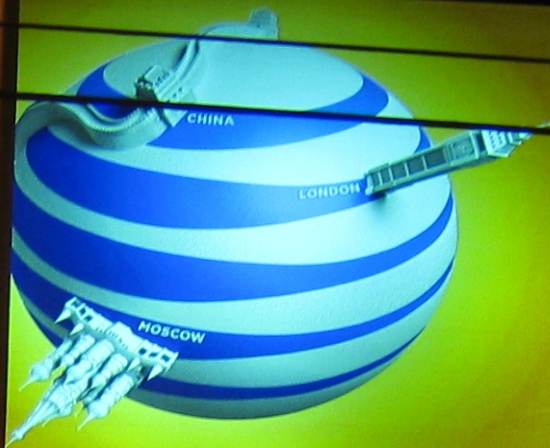



Surveillance

Beyond circumvention



AT&T works in more places,
like **NSA HEADQUARTERS**

The new  at&t

#951545

 CBS

14'h x 48'w

USED CARS
ECITY MOTORS, Inc.
415-626-6363
www.ecitymotors.com

14TH ST
FOR CARS



PUBLIC
WALKING

zipcars

What is the purpose of Surveillance?

- In short:
 - Linkability for the purposes of ...
 - Massive data gathering in the pursuit of...
 - Social and economic control
 - Enforcement of power structures

How does it work?

- Personal Surveillance Machine
 - Your telephone – the more you pay - the better it watches you; who needs smart kids when we've got smart phones?
- The internet
 - People think censorship is surveillance; censorship is merely a symptom
 - Data retention is silent
 - Nearly everything falls in the face of infinite memory; a system that never forgets? Never.

Lawful interception

- Purposeful technical compromise is literally an unacceptable compromise; we must not buy the lie that backdoors make us safer – it is a farce!
 - How many CALEA systems are compromised?
 - How many network monitoring systems?
- Companies are forced to become the police without even so much as a thought to due process
- Every service is exported to those gagged by the “law”
 - Defense isn't even an option; we have no knowledge
- Police do not understand the world they are building
 - We do; we must make their efforts futile. They do not see the big picture; we must create a better picture

Syria

- Syria is the internet wet dream of authoritarians
- Blue Coat is a major weapon of choice
 - Produced in the West for the “Free Market”
- Internet cafes are keylogged; tied to national ID
- Full packet logging at borders and internally
 - Snort and custom software
- DNS filtering for an alternate reality
- Windows 2003, Syscache, Packeteer, etc
- Crypto for the privileged not for others
- Still imperfect and very heavy handed

Tactical and strategic exploitation

- A reality and a sad, scary one at that
- FinFisher, RCS from HackingTeam, R2D2 exposed by the CCC, many many others
- These guys are arms dealers and they know it
- We must **ruin** it for them
 - Disclose their backdoors
 - Disclose their techniques
 - Disclose the payloads
 - Discredit them
 - Expose their personnel; name and shame
 - Demonstrate their ethics to the public; follow the money

A realistic approach

- Privacy by policy is a failure
 - All policies are based on promises without technical or even social ability to understand compromise
- The law is unable to protect or adapt
 - It may be able to slow or contain some things; doubtful
 - Illegal methods will simply lead to anonymous tips and the use of legal methods
 - Without by-default strong anonymity, individuals are targeted – in databases and/or real time attacks

Privacy by Design

- What is privacy anyway?
 - It is a kind of understanding
 - It is autonomy and power; it is individual agency
- What is Privacy by Design?
 - Isolation and Compartmentalization
 - Quantify systems into pieces with known bounds
 - Detection of abnormal behavior
 - Minimize functions and information as much as possible
 - Requires no knowledge by the user to do the Right and the Safe Thing(s)

Cryptography only buys us time
it is not a panacea

At the core

- The world has changed into a network mediated global society
- The global society is mediated by core networks
- The core is rotten
 - In Sweden it's the FRA – legal and rotten despite legal hand-waving
 - We must treat the network as hostile and compensate

Why? What's the big idea?

Intention and activities

- What do people do?
- How are they doing it?
- Why are they doing it?

People communicate

- The protocols and applications they used are insecure
 - They use their phone
 - SS8 builds a backdoor; the phone company deploys it
 - They use IM on their computer
 - HackingTeam compromises the computer; installs RCS
 - They encrypt their drive
 - FinFisher extracts their computer's memory
 - Or they are forced by law to incriminate themselves
 - They browse the web
 - Everyone profits from tracking
 - Every browser is a security nightmare

What do people expect?

- “Security” and “privacy” are actually simplifications of complex interactions; expectations that are never really expressed except as abstract ideas
- Generally users hope for the following:
 - That the network is as friendly as their daily lives
 - That the people in charge will bring just
 - That things will be taken care of for them
- Probably most realistically, people pessimistically expect *nothing*; closer than most to reality

Prerequisites for a chance

- Open standards
- Open designs
- Decentralized designs over centralized
- Free Software
- Free Hardware
- Perfection is the enemy of good enough
 - Change the value; economics of scale matter
 - Strive for a kind of perfection *anyway*

Social networking

- Crabgrass is a step in the right direction
 - Free Software as private as possible with centralization
 - Exists today
 - <https://we.riseup.net>
- Diaspora is another step in the right direction
 - Free Software but still complex
 - Sorta exists today but is largely beyond normal people; lacks the network effect

SSL/TLS

- Broken trust and bad crypto in *reality*
- Better than nothing? Probably – could use a redesign
- We must ensure that people use ephemeral ciphers and modes
- We need a real solution to the CA trust model
 - The work by Adam Langely
 - HTTPS-Everywhere
 - Collection/Detection of anomalies
 - HSTS, etc
 - Convergence
 - Trust agility as Moxie says

Off-The-Record (OTR)

- Instant messaging
 - Forward secrecy with deniability
 - Even if someone is logging - the data is reduced to frequency and relationship information; not content
- Libotr
 - Integrate it into everything
 - Audit it for bugs
 - Make it easier to use
 - Improve it with research, key sizes, obfuscation, timing channels, etc
- Make new implementations

PGP/OpenPGP?

- If you must use a store and forward medium and OTR won't cut it – use PGP
- It lacks a core feature of OTR
 - Forward secrecy
 - This is a *disaster*
- It is impossible to use for basically everyone
- Key signing used for social network analysis by cops
- OpenPGP smart cards are probably better than nothing; we need free software firmware – perhaps Werner will release his someday?

ZRTP

- Encrypted voice and video is really badly needed
 - Forward secrecy
- ZORG is free software (!) for ZRTP
- PrivateGSM
 - Practical multi-platform encrypted calling
- RedPhone
 - A similar Android only approach
- We need ZRTP built into *everything* that does voice and video calling; the above two are good enough but far from perfect

Tor

- An anonymous communication system for transporting other protocols
- Part of the present – mutual aid for resisting the damage inflicted by a surveillance enabled infrastructure
- Forward secrecy with strong crypto
- Open standards, Free software
- It's not perfect but it beats everything else hands down; a real Privacy by Design system
- We want you to help with *everything*

The Torouter

- An incentive based idea for helping to drive adoption
- An idea with working code
- Based on Debian Gnu/Linux
- All Free Software
- We hope to add other software into the mix as we go along – TahoeLAFS and similar privacy by design software

Obligatory hardware visual



(Please look at the front of the room for a hardware example based on DreamPlug – much like the Freedom Box...)

Torouter features

- Transparent Torification of your entire network
 - Route all traffic over Tor; drop anything that can't be anonymized
 - Create a Tor bridge even behind a NAT (when possible)
 - Create Tor relays when desired
 - Replace that proprietary NAT device
 - Take back control of your core
 - Free and Open Wifi – routed over Tor – help your neighbors and the neighborhood

Torouter hacking

- We need Web UI hackers, security auditing, hardware designers – the works
- Translation, feedback from non-technical users – anything helps

Driving adoption through normalization

- Normalization key; expected norms rule
- Integration of Privacy by Design systems
- Anonymity as the strong default
- We must make dragnet surveillance worthless
- We must obscure relationship information as far as the network is concerned
 - The physical network connecting to the internet
 - The logical network connecting everyone together
 - We must return agency to every person

Hope for activities online?

- Group text chat – mpOTR?
- Group voice chat – ZRTP someday?
- File sharing – TahoeLAFS, Tor Hidden Services, GnuNet – today
 - In the future? OpenSWARM, anonymized torrenting with stronger crypto?
- The Freedom Box – someday?
- Blocking of anonymity systems – Telex or other decoy routing systems someday?

So you want to help with
circumvention?

Think beyond circumvention

(Sure you should also run a Tor bridge or relay)

Questions?