Privacy as Security

Dr George Danezis

Microsoft Research,
Cambridge, UK.
gdane@microsoft.com

Key Thesis and Outline

What is this talk about?

- Explore the relations between notions of ‘privacy’ and ‘traditional security’.
- Key thesis: **Privacy is better understood as security**!

How do we proceed?

- Introduction to Privacy.
- Revisiting security/privacy properties.

Scope

Ground rules of this talk:

- **High-level**: keep out the very technical details. Implementation issues, system specific, cryptography, statistics, standards.
- Focus on **technology** and **technology policy**. There is also law, sociology, political science, and politics.
- Look at privacy in the context of **computer security** Security properties, adversary models, security policies, . . .
- A clear focus on the **real world** and its constraints.

Caricature of the debate: Security *or* Privacy

"Privacy" important but. . .

- . . . what about abuse and accountability?
- . . . difficulties for Law Enforcement?
- . . . copyright or libel?
- (. . . what does a good, honest person has to hide anyway?)

Established wisdom:

- Need for a *balance*. . .
- Control/limit *dangerous* technology (or research).
- Result: Surveillance by design → no privacy (often).

Caricature conclusion: *Security* is most important!

Security *and* Privacy in Context

A brief history of security, and where does privacy fit?

- Early days (Pre-1970s): **Security for the Government and Military**. Focus on confidentiality properties. Some work on Tamper resistance, signal intelligence, . . . Keep secrets using computer security.
- 70s to 90s: **Commercial security** and security for enterprises. Focus on integrity and authenticity, bank transactions, contracts, audits, signatures.
- 90s to today: **Security for households, citizens, civil society**. Most computers get networked, and everyone start having their security worries. With limited budget, and no army of any type. . .

The era of **Privacy Concerns**.

Privacy *is* Security (I)

Privacy is **Informational self-determination**:

- Giving out less information
- Gaining more control over one's informational environment.

Why is it important?

- Privacy satisfies valid *security* needs of some entities. Examples: freedom from surveillance and profiling, flexibility to access and use content and services, freedom from compulsion, . . .
- Small(ish) entities: no serious means to gain assurance.

Privacy *is* Security (II)

Who are the small entities?

- Households and individual citizens.
- NGOs, civil society, . . .
- Small companies with no tech department?
- Small(ish) governments?

Shared infrastructure:

- Despite varying capabilities infrastructure is shared.
- Telecommunications, operating systems, search engines, on-line shops, software, . . .
- **Denying security to some, means denying it to all**.

Privacy *is* Security (III)

Like all security, privacy must be technologically supported:

- Privacy/security needs cannot just be satisfied with good intentions.
- Laws are necessary but not sufficient to protect privacy/security.
- Technology must provide assurances where possible – procedures and audits where it is not.

Hence the development of **Privacy Enhancing Technologies**.

Where next?

Present some interesting privacy/security properties:

- How the standard security properties can be fortified for privacy.
- New concepts that are antithetical to current security practices.
- Why are privacy properties useful?

At the beginning there was *Authentication*

Early work on security focused on authentication – the fist step before any security policy can be applied.

- Makes sense in a government, commercial or military context.
- But does it make sense when you do not have a closed and known user group?
- PET: from Authentication to **Identity Management**.

Privacy preserving Authentication mechanisms:

- Private Authentication: to protect against 3rd parties.
- Anonymous Credentials: to protect against all.

Private Authentication

How does authentication traditionally works:

- (Alice) → (Bob): Hi all! I am Alice, and I think you are Bob, and here is some crypto stuff.
- (Bob) → (Alice): Hi Alice, Bob here! ...

Private Authentication:

- This is a problem.
- Solution: hide from third parties Alice or Bob's identity.
- Hiding both Alice and Bob is a bit more tricky.
- Failed authentication should not give out any information about either.
- When both have multiple identities even more tricky.

State of the art: Just Fast Keying,...

Anonymous Credentials

Aim: gain privileges by proving that you have some attributes, according to some authority, without revealing any identity.

- Players (Cinema Scenario): Authority (the box office), Prover (spectator), Verifier (ticket verifier).
- Traditional security equivalent: anonymous capabilities.

The state of the art:

- Any string or number as an attribute.
- can prove arbitrary boolean statements on attributes
- can prove range statements.
- Double spending and velocity checks.

Downside: Heavy crypto and patents. Multishow (IBM), Single show (Chaum,Credentica).

“The Secure Channel” and privacy

Commonly deployed security mechanism.

- A success story – what we can do well!
- Widely deployed for messages and streams.
- Examples: PGP, SMIME, SSL, SSH, IPSec, . . .

A closer look at the properties:

- Authenticity – we talked about this before.
- Confidentiality – no third party should be able to read it.
- Integrity – no third party should be able to modify it.
- (Non-repudiation) – you should not be able to deny what you said.

Off-the-record security

Traditional view good for the military/commercial world:

- Key management can be done safely.
- Transactions are archived and can be used in court.

What about instant messaging? Keep things *Off-The-Record*.

- Examples: Briefing a journalist, talking on the phone to your lawyer or friends.
- **Plausible Deniability** (not non-repudiation): no one can prove you said something.
- **Forward secrecy**: once the communication is securely over, I cannot decrypt it any more.
  (**Freedom from compulsion**.)
- Still want Authenticity, Confidentiality and Integrity.

State of the art: OTR plug-in for IM.

Secure *Anonymous* channels (I)

Key questions and properties:

- Should anyone know with whom I am talking?
  (**3rd party anonymity**.)
- Should the website I am visitng know who I am? And correlate my visits?
  (**Sender/Initiator anonymity**.)
- Should those who want to contact me know who I am/where I am?
  (**Receiver/Server anonymity**.)

Applications: Voting, e-cash, security alert gathering and monitoring.

State of the art: Java Anon Proxy, Tor, Mixminion, (Anonymizer).

Secure *Anonymous* channels (II)

More generally: **freedom from traffic analysis**?

- TA can be used to extract information – particularly from streams of data.
- TA can be used for **target selection**:
  Which laptop to steal? Which house to break in? Which server to attack?
- Mobile world: **Location privacy** is becoming a problem.

State of the art: *(this space is left intentionally blank.)*

Compulsion Resistance

Forward security:

- After some time/steps no one should be able to compromise the security properties.
- Protection under physical pressure / blackmail.

Other forms of compulsion resistance:

- Election schemes need ‘receipt freeness’.
- Steganographic file systems: Under compulsion you can reveal some files, but hide others.
- Safebox folders: you can put data in, but not decrypt it until you are back home.

Open challenge: Data Sharing

To buy things and get services you need to share data:

- Payments, delivery addresses, system configuration, . . .
- Often with more powerful entities, and little choice.
- Once your data is out there, how to protect it? How to control its use?

Data protection regimes:

- EU/Canada/Australia impose standards.
- Violations are well funded and technologically supported, enforcement is underfunded and non-technological.
- Need more automatic audits, Chinese firewall policies, design of privacy friendly architectures, standard protocols. Integration of privacy in the overall s/w process.

The new *availability*: censorship resistance

Privacy links with Peer-to-Peer computing:

- Massive resilience: perfect for weak nodes.
- No a-priory centralisation – only loose coordination.
- Obvious first application: communicate and share information.
- Popularity due to hostile environment (security/resilience.)

Reputable and marketable applications:

- Efficient and resilient distributed systems.
- Robust and cheap delivery: Bit-Torrent.
- Bridging NATs: Skype – firewall piercing modes of Tor.
- The future: Social Networking / Expert finding. . .

Abuse Resistance is a PET enabler

Privacy and security policies and **countermeasures to abuse**.

- Credentials: double spending for coins, private black listing for abusers.
- Bulletin Boards: Social network based reputation, ranking of articles, moderation.
- Peer-to-peer: Sybil attack resistance.

The dangers of ‘escrow’ or ‘revocable privacy’:

- Why would you trust the revocation authority?
- Abstract designs are a poor match for the real world.
- Include the revocation process into the security model, and judge its robustness to abuse. Impose *technical* checks and balances. Demand efficient and automated audits.
- **Just say no**.

Some Conclusions. . .

A fresh view of privacy:

- Self-determination: the most valued security property.
- Privacy should become a **first class security property**.
- Use tools from security engineering.

Challenges and opportunities:

- Properties also benefit enterprises, governments and overall strengthen infrastructure.
- High assurance circles: traffic analysis, location anonymity, compulsion resistance already requirements.
- Data Sharing assurances must be integrated in the process. Novel technical support badly needed.
- Abuse control: solutions outside the (escrow) box.

. . . and pointers.

- Any questions?

- Contact me: George Danezis `gdane@microsoft.com`
- Fund and attend the Privacy Enhancing Technologies Workshop, Leuven, July 2008.