Towards Accountable Anonymity

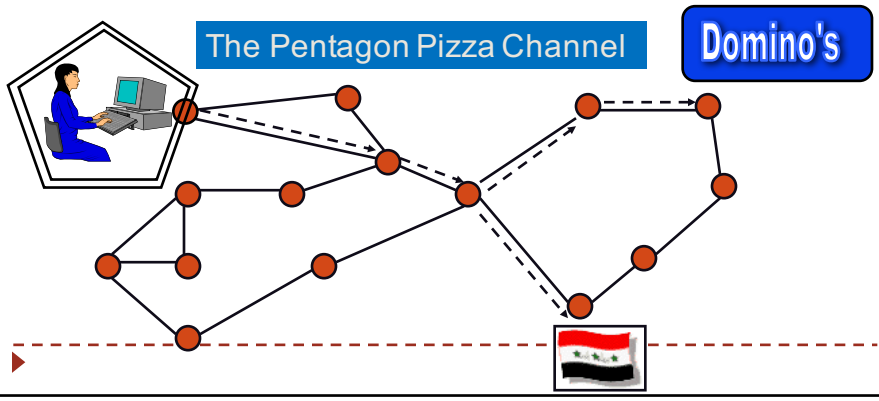
Yong Guan

Department of Electrical and Computer Engineering
Associate Director for Research, Information Assurance Center
Iowa State University

August 5, 2016

Preliminary: Anonymity & Pseudonymity

- Req: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms
  - David Chaum
- Req: An Optimal Strategy for Anonymous Communication Protocols
  - Y. Guan, X. Fu, R. Bettati, and W. Zhao



IOWA STATE UNIVERSITY

Preliminary: Anonymity & Pseudonymity

- Anonymizing Channels vs. Anonymizing Data

A number of Anonymous Communication Systems have been realized. Several well-known systems are:

- **Anonymizer** (anonymizer.com)
- Anonymous Remailer (MIT LCS)
- **Crowds** (Reiter and Rubin)
- Freedom (Zero-Knowledge Systems)
- Hordes (Shields and Levine)
- **Onion-Routing** (NRL)
- PipeNet (Dai)
- SafeWeb

IOWA STATE UNIVERSITY

Anonymizer

- User connects to the proxy first and types the URL in a web form
- Channels appear to come from proxy, not true originator
- May also filter traffic for identifying information
- It offers encrypted link to the proxy (SSL or SSH)

IOWA STATE UNIVERSITY

Chaum Mixes

Invented by David Chaum

- as were DC-nets, blind signatures, and most of the building blocks of anonymity technology

Underlying Idea for Mixmaster remailer, Onion Routing, ZKS Freedom, Web Mixes

Basic description: A network of mix nodes

- Cell (message/packet) wrapped in multiple layers of public-key encryption by sender, one for each node in a route
- Decrypted layer tells mix next node in route
- Mixes hold different cells for a time and reorder before forwarding to respective destinations

IOWA STATE UNIVERSITY

Mix Options

Basic Routes

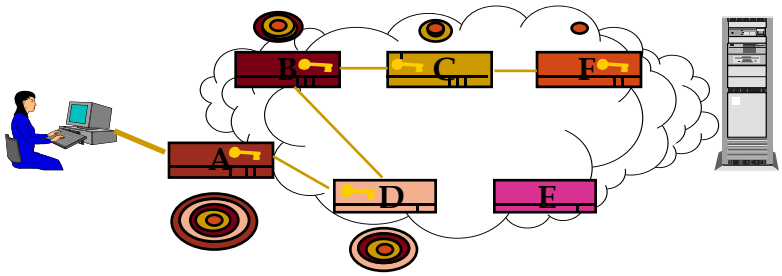
- Mix Cascade: All cells from any source move through a fixed order "cascade" of mixes
- Random route: Route of any cell is selected at random by the sender from the available mixes. (Sometimes "mix network" reserved for this case.)

Basic Flushing (reordering and forwarding cells at a mix)

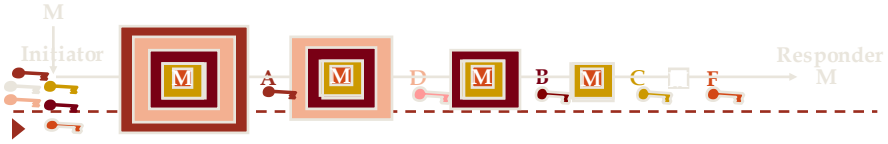
- Threshold Flush: Mix flushes all cells whenever a threshold number of received cells is reached
- Pool Flush: Mix flushes each cell with probability p whenever a threshold pool size of received and existing cells is reached
- Time-slice Flush: Mix flushes all cells it holds every t seconds
- Stop and Go Flush: Sender chooses (random) time for cell to be held at each mix

IOWA STATE UNIVERSITY

Onion Routing



- The initial proxy knows the Onion Routing network topology, selects a route, and generates the onion
- Each layer of the onion identifies the next hop in the route and contains the cryptographic keys to be used at that node.



IOWA STATE UNIVERSITY

Dining Cryptographers (DC) Networks

- Req: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability
  - David Chaum
- Req: The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability
  - Michael Waidner and Birgit Pfitzmann

Dining Cryptographers (DC) Networks

Their waiter comes in and tell them: Someone has paid this dinner for you!

IOWA STATE UNIVERSITY

Anonymity ←→ Accountability?

- Anonymous systems: the ring of Gyges in cyber world.

- Well-known online anonymity services
  - Tor
  - Anonymizer
  - ….

- Use of Tor

Family & Friends

Businesses

Activists

Media

Military & Law Enforcement

IOWA STATE UNIVERSITY

Problem: Malicious/Criminal Uses of Tor

- Online "Invisibility": This kind of anonymity is absent of restraint and responsibility:
  - Anonymous attacks (Feb. 5, 2013, ABC news)
  - Threatening emails/VoIP calls
  - German child pornography case (use of Tor) in September 2006, where the investigation was stymied by the authorities' inability to reveal the content distributors.
  - Darknet marketplace - The Silk Road (2011 Summer, use of Tor, over $20 Million in annual sales): "features pictures of various drugs for sale – including heroin and cocaine - and allows buyers to place them in a shopping cart, similar to those on Amazon and other consumer sites".

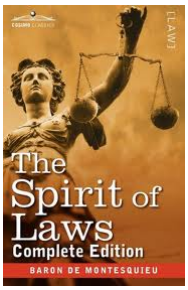
IOWA STATE UNIVERSITY

How to Make "Criminal Use of Tor" Accountable

- We can easily see that Anonymity systems like TOR, although not purposefully supportive of criminals, is being utilized, via this Dark Net construct, to host a myriad of illegal activities.
  - A real stumbling block to network forensics professionals, and especially to Law Enforcement, in their pursuit of cyber criminals on the Internet.

IOWA STATE UNIVERSITY

Our View



The need for Accountability in the context of Anonymity.

- Anonymity is primarily reflections of liberty.
- Absolute liberty is not rational in real world.
- We believe anonymity is not absolute.

IOWA STATE UNIVERSITY

"Liberty means responsibility. That is why most men dread it."

— George Bernard Shaw

IOWA STATE UNIVERSITY

Accountability vs. Anonymity

- We show that although accountability appears to impair anonymity, there is a possible way that can combine anonymity and accountability into one framework.

IOWA STATE UNIVERSITY

The Concept of Accountable Anonymity

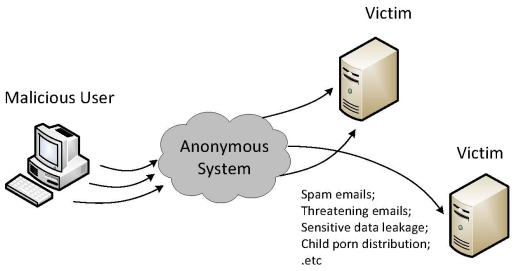
- Here, we introduce a new concept "Accountable Anonymity":

- Accountable Anonymity is achieved when the following features are implemented simultaneously:
  - Users enjoy anonymity under normal circumstances;
  - Under certain circumstances, the source could be traced without impairing others anonymity;
  - The accountable protocol is incentive-compatible;
  - It is infeasible to frame or impersonate an honest user.

IOWA STATE UNIVERSITY

Threat Model

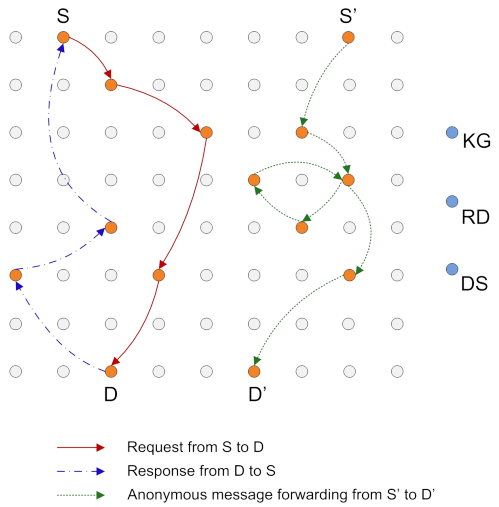
- Anonymity is provided in the sense of preventing attackers from linking communication partners.
- Our accountable mechanism only addresses the cases where good users are attacked by bad users, for example after a threatening email is received.



IOWA STATE UNIVERSITY

Accountable Anonymity

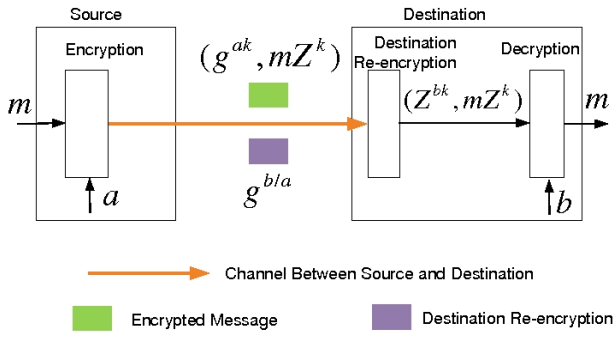
We show the design of the 1st anonymous system providing Accountable Anonymity.



IOWA STATE UNIVERSITY

Implementation for Accountability

- If both S and D are registered and the keys cannot be forged, S is accountable and is forced to follow the protocol.
- Otherwise, D cannot decipher/read the message.



IOWA STATE UNIVERSITY

Four Phases

- Setup phase: Initializes our system and sets up the basic environment.
- Join phase: Initializes a node who wants to use the Accountable Anonymity service.
- Communication phase: Achieves the regular anonymity.
- Forensic investigation phase: is limited to identifying the source of the cyber criminals, only when appropriate legal procedure is followed.

IOWA STATE UNIVERSITY

Join Phase

- User S produces his secret key $sk_S = \theta_i \in Z_q^*$ and interacts with KG and RD.
- S makes $\{ID_S, g^{\theta_i}\}$ published by RD; gets an encryption key g^{θ_i/π_i} , π_i and one of the decryption keys $dk_2 = S(g^{\pi_i/\theta_i})$.
- RD obtains a piece of masked tracing information $\{ID_S, g^{\theta_i}, g^{\sigma\pi_i/\theta_i}\}$. σ is KG's secret.

A user S can only be revealed with multiparty cooperation.

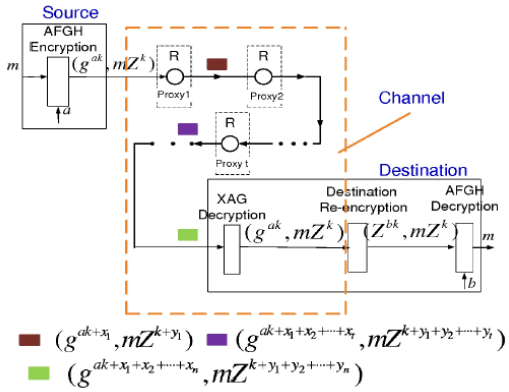
IOWA STATE UNIVERSITY

Communication Phase

- S generates destination re-encryption key $dk_3 = g^{\pi_i\theta_j/\theta_i}$ from D's published information $\{ID_D, g^{\theta_j}\}$.
- Once encrypted, the message can be decrypted only with both the destination re-encryption key and D's secret key.
- S generates packets. A packet including an onion header and payload.
- Routing Information and re-encryption keys for the intermediate proxies are distributed by the onion header.

IOWA STATE UNIVERSITY

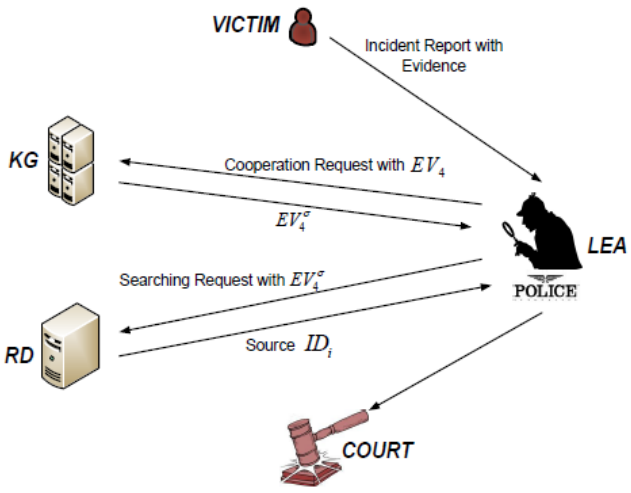
Communication Phase



- The communication channel is provided by the scheme I.
- The scheme II provides for logical communication between the source and destination.
- In the schematic, $a = \theta_i/\pi_i, b = \theta_j$.
- The destination re- encryption key is $dk_3 = g^{\pi_i\theta_j/\theta_i}$.
- dk_4 is the signature.

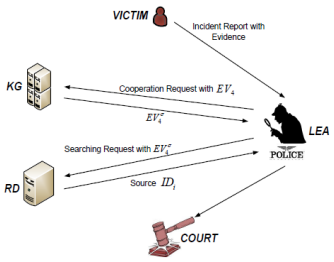
IOWA STATE UNIVERSITY

Forensic Investigation Phase



IOWA STATE UNIVERSITY

Forensic Investigation Phase



1. The victim sends to LEA a report along with collected evidence.
   $EV_1 = m, EV_2 = mZ^k, EV_3 = \alpha/g^{dk_0} = g^{\theta_i k/\pi_i}$
   $EV_4 = g^{\pi_i/\theta_i}, EV_5 = S(g^{\pi_i/\theta_i}), EV_6 = dk_4.$
2. LEA verifies:
   - m is malicious.
   - EV_5 is a valid KGs signature on EV_4.
   - $EV_2/e(EV_3, EV_4) = EV_1$.
   - EV_6 is a valid digital signature of EV_2, EV_3 using EV_4
3. LEA provides $EV_4 = g^{\pi_i/\theta_i}$ to KG and asks for cooperation.
4. KG processes it and gives converted evidence $EV_4^\sigma = g^{\sigma\pi_i/\theta_i}$ to LEA.
5. LEA then sends it to the RD with a subpoena.
6. The source of the malicious message is found by searching RDs database (checking in which tuple $\{ID_S, g^{\theta_i}, g^{\sigma\pi_i/\theta_i}\}$, EV_4^σ appears).

A user can only be revealed with these multiparty cooperation.

IOWA STATE UNIVERSITY

Next Steps

Problem we solve:

Up to now, there is no good solution against illegal uses or abuses in current anonymous systems.

We propose to design an anonymous system with accountability:

- it provides anonymity to law-abiding users
- under certain circumstances, it can trace the source of illegal uses and abuses

More challenging future work:
Run it as a service on Internet.

IOWA STATE UNIVERSITY

Thanks

Q&A

Yong Guan
guan@iastate.edu
Iowa State University