Slide 1

IK1552 Internetworking/Internetteknik

prof. Gerald Q. Maguire Jr. http://people.kth.se/~maguire/

School of Electrical Engineering and Computer Science (EECS), KTH Royal Institute of Technology

IK1552 Spring 2019, Period 4 2019.04.07

Slide 2

Module 13: Communications when others are (probably) listening

Lecture notes of G. Q. Maguire Jr.

Slide 3

Context

Edward J. Snowden's leak of government documents revealed extent of interception & active attacks

June 2014 - :

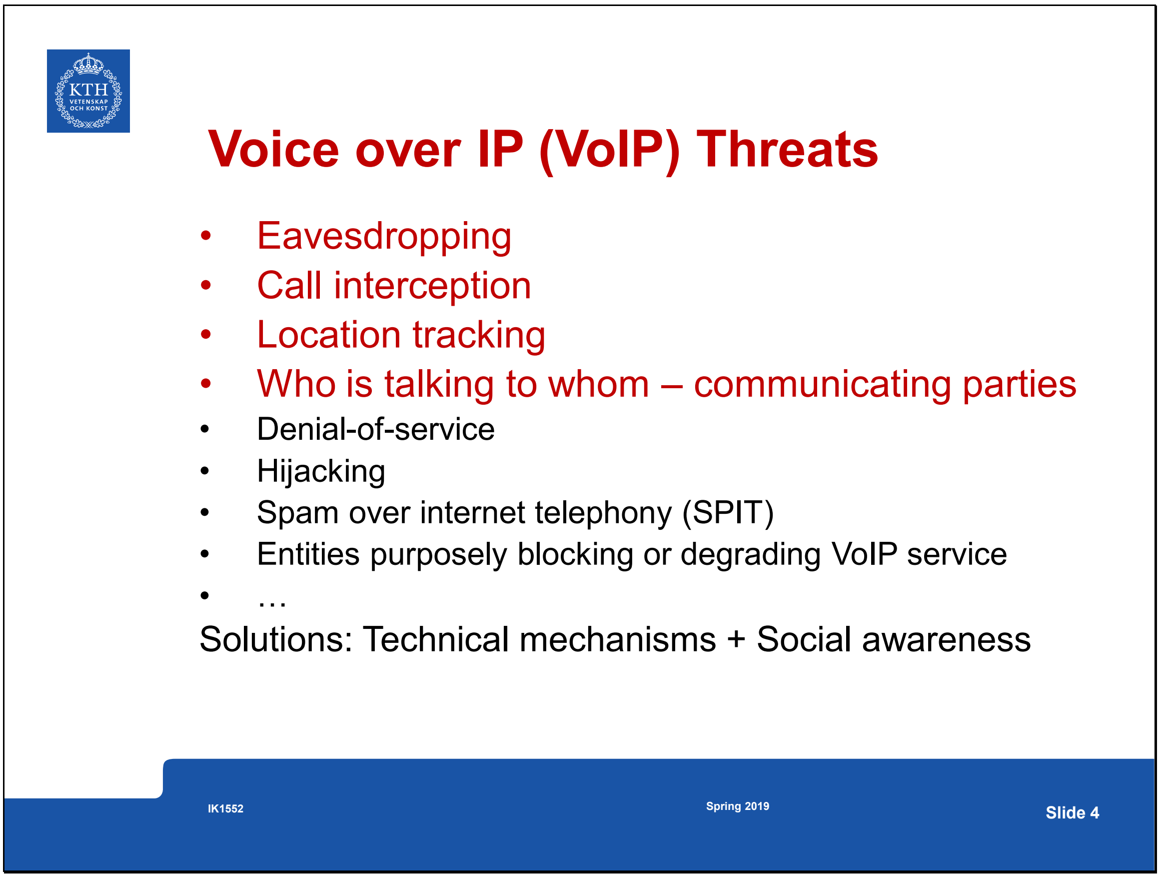
- http://www.washingtonpost.com/world/national-security/nsa-secrets/
- http://www.theguardian.com/us-news/the-nsa-files
- http://www.spiegel.de/international/germany/new-snowden-revelations-on-nsa-spying-in-germany-a-975441.html

There is no question that there are people listening, be it the U.S.'s NSA, Sweden's FRA, France's DGSE , … There are also private persons and businesses that are listening.

> See for example the romantic messages intercepted between personnel on Sweden's HMS Vinga and HMS Ulvön that was intercepted by radio amateurs and released on the Russian site Radio Scanner (http://www.thelocal.se/20141128/russia-intercepts-sweden-navy-love-texts)

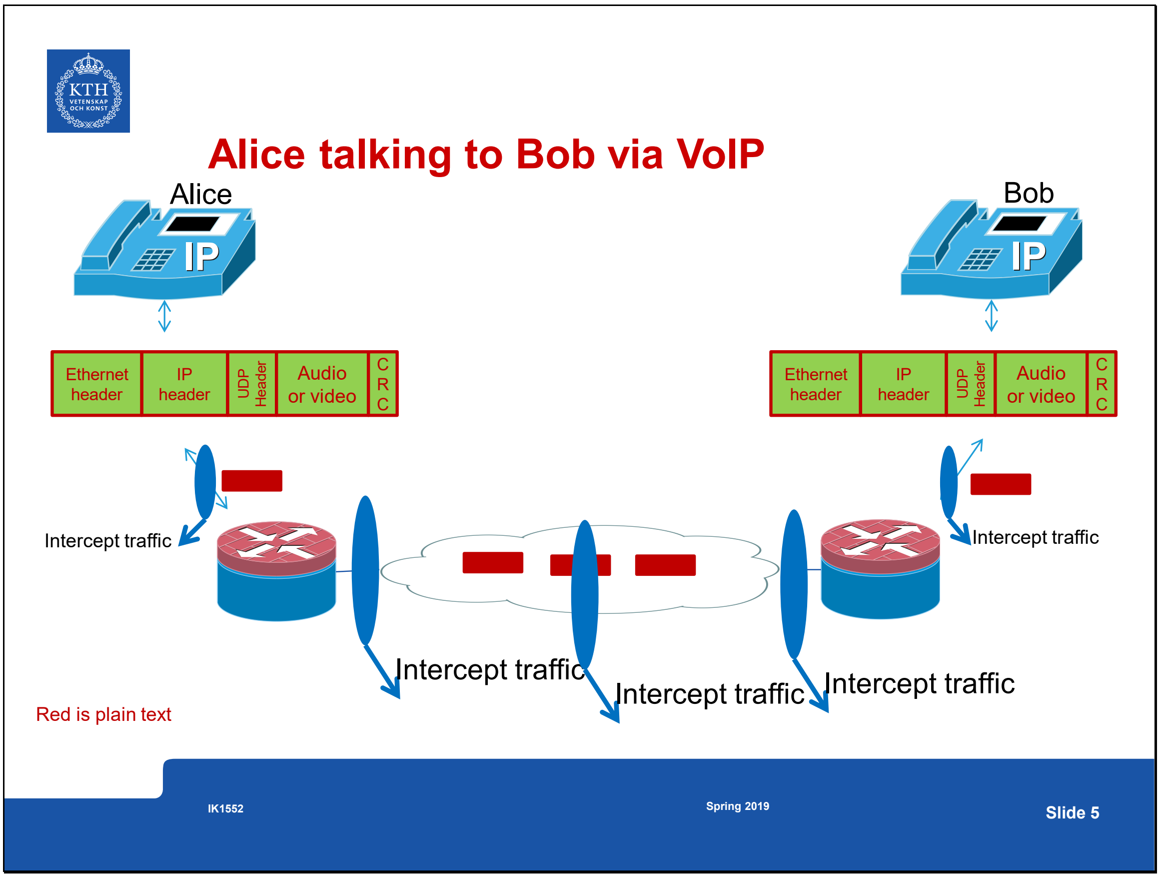
KTH Crosstalks – "The dark side of the web - Internet's parallel universe"
https://www.youtube.com/playlist?list=PL3k3XLxxiiaYZoYhbvCZso5sOETvqMSzH
http://crosstalks.tv/dark-networks-not-necessarily-evil/

Slide 4



March 2014 lecture

Slide 5


Alice talking to Bob via VoIP
Alice
Bob
IP
IP
Ethernet header
IP header
UDP Header
Audio or video
CRC
Ethernet header
IP header
UDP Header
Audio or video
CRC
Intercept traffic
Intercept traffic
Intercept traffic
Intercept traffic
Intercept traffic
Red is plain text
IK1552
Spring 2019
Slide 5

Slide 6

What is "meta data"?

- Meta data is the data about communications – as opposed to the content of the communication
- In traditional telephony this would include:
- Caller and callee phone numbers, time of day, and duration
- Cellular telephony meta data may include base station ID, geolocation of the terminal, IMEI, …
- Internet communication: source & destination IP addresses, protocol, source & destination port numbers, and other header information.

IK1552 Spring 2019 6

Slide 7

Meta data and IPv6

Is an IPv6 header meta data or content?

0	4	8	12	16	20	24	28
Versio n	Traffic class		Flow label				
Payload length				Next header		Hop limit	
Source address							
Destination address							

Slide 8

Meta data and IPv6

Alberto Escudero-Pascual’s 2002 licentiate thesis ‘Privacy in the next generation Internet. Data protection in the context of European Union policy’ argues that some of the header is **content** and not simply meta data

IPv6 with autoconfiguration ⇒ unique identifier based upon the MAC address of the interface you are using

Network prefix + 64 bit identifier

- Reveals your MAC address
- With DB of vendor IDs can reveal what kind of device you are using
- The 64 bit identifier does not change when you move from net to net

⇒ Cryptographically Generated Addresses (RFCs 3972 and 4581) and Secure Neighbor Discovery (SEND) protocol (RFC 3971)

IK1552 Spring 2019 8

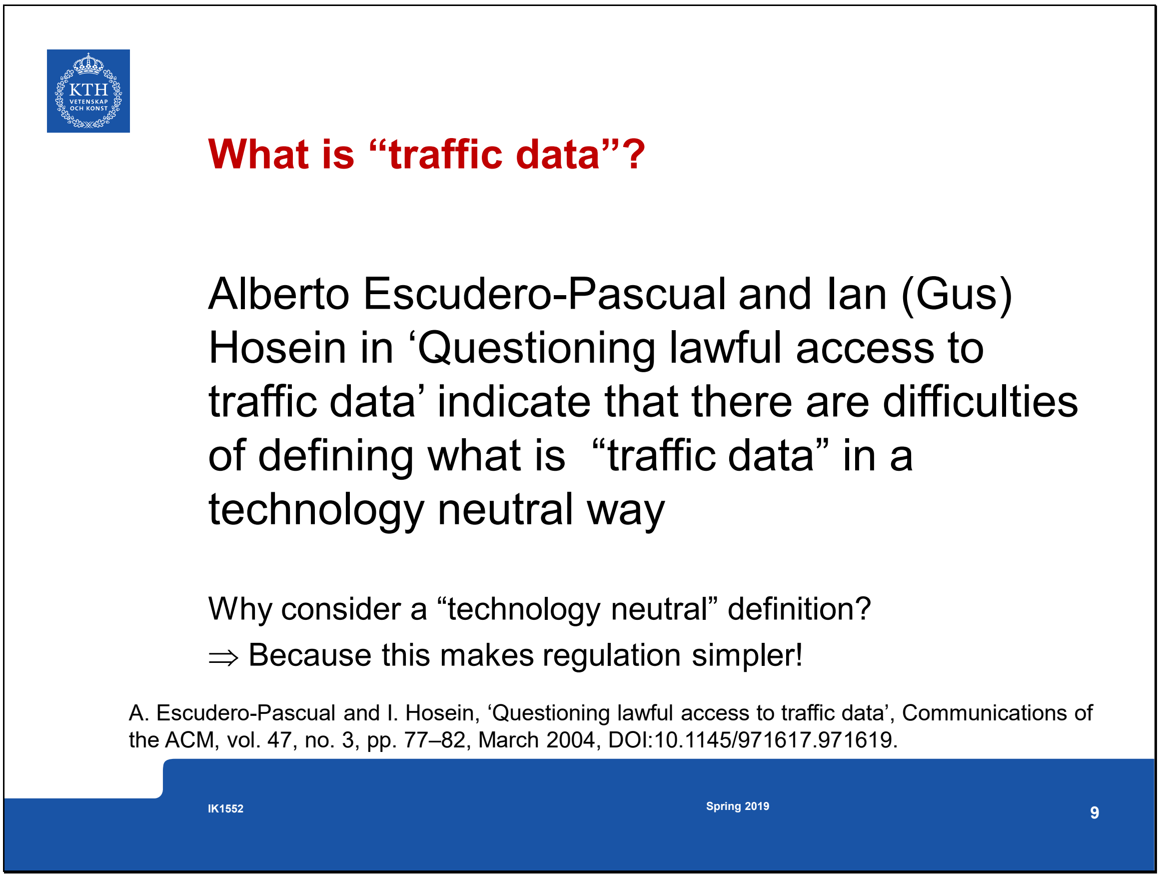
A. Escudero-Pascual, ‘Privacy in the next generation Internet. Data protection in the context of European Union policy’, KTH, Microelectronics and Information Technology, IMIT, 2002. http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-3435

T. Aura, ‘Cryptographically Generated Addresses (CGA)’, Internet Request for Comments, vol. RFC 3972 (Proposed Standard), March 2005, Available at http://www.rfc-editor.org/rfc/rfc3972.txt

M. Bagnulo and J. Arkko, ‘Cryptographically Generated Addresses (CGA) Extension Field Format’, Internet Request for Comments, vol. RFC 4581 (Proposed Standard), October 2006, Available at http://www.rfc-editor.org/rfc/rfc4581.txt

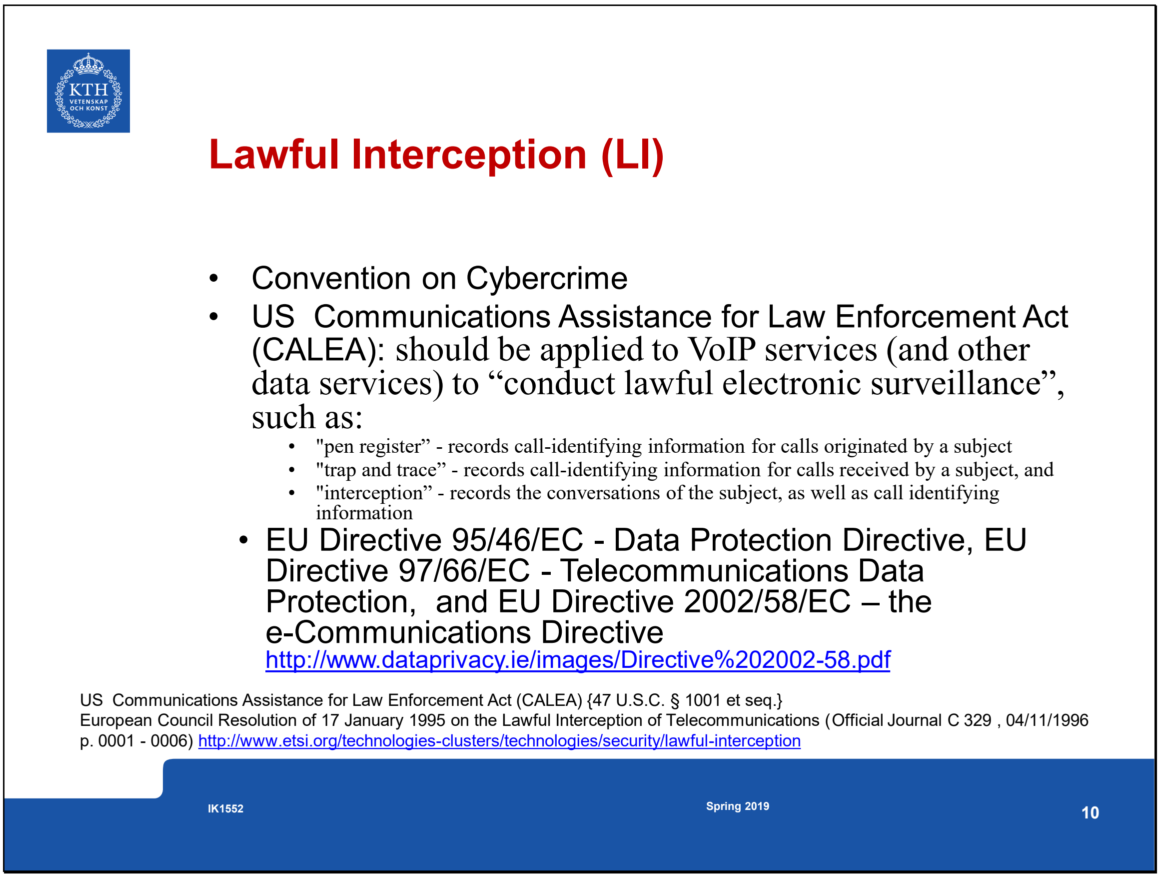
J. Arkko, J. Kempf, B. Zill, and P. Nikander, ‘SEcure Neighbor Discovery (SEND)’, Internet Request for Comments, vol. RFC 3971 (Proposed Standard), March 2005, Available at http://www.rfc-editor.org/rfc/rfc3971.txt

Slide 9



A. Escudero-Pascual and I. Hosein, ‘Questioning lawful access to traffic data’, Communications of the ACM, vol. 47, no. 3, pp. 77–82, March 2004, DOI:10.1145/971617.971619.

Slide 10



US Communications Assistance for Law Enforcement Act (CALEA) {47 U.S.C. § 1001 et seq.}

European Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications (Official Journal C 329 , 04/11/1996 p. 0001 - 0006) http://www.etsi.org/technologies-clusters/technologies/security/lawful-interception

Slide 11

FRA law (FRA-lagen in Swedish)

Government proposal 2006/07:63 – Changes to defence intelligence activities (Swedish proposition 2006/07:63 – *En anpassad försvarsunderrättelseverksamhet*).

Authorizes Swedish National Defence Radio Establishment (*Försvarets radioanstalt* (FRA)) to intercept traffic crossing Sweden's borders

Mark Klamberg, "FRA and the European Convention on Human Rights - A Paradigm Shift in Swedish Electronic Surveillance Law", Dag Wiese Schartaum (editor), Overvåking i en rettstat in the series Nordisk årbok i rettsinformatikk (Nordic Yearbook of Law and Information Technology), Fagforlaget, Bergen 2010, pp. 96-134. http://www.diva-portal.org/smash/get/diva2:390333/FULLTEXT01.pdf

IK1552 Spring 2019 11

Mark Klamberg, "FRA and the European Convention on Human Rights - A Paradigm Shift in Swedish Electronic Surveillance Law", Dag Wiese Schartaum (editor), Overvåking i en rettstat in the series Nordisk årbok i rettsinformatikk (Nordic Yearbook of Law and Information Technology), Fagforlaget, Bergen 2010, pp. 96-134

http://www.diva-portal.org/smash/get/diva2:390333/FULLTEXT01.pdf

Slide 12

FRA monitoring communications since 1930s

"Clarification: In the SOU (Swedish Government Official Reports) 2009:66 Signalspaning för polisiära ändamål (signals intelligence for law enforcement purposes), p. 55 it is stated that the police started with signals intelligence 1939. The Defence Radio Establishment (FRA) was established 1942 (its predecessor already in 1937). Professor Agrell has found documents in the archives of the Swedish state that show that the Swedish Government in a secret decision in 1948 obligated Telegrafstyrelsen (government-owned corporation, public enterprise, responsible for telecommunications) to transfer all telegram destined or from foreign embassies to the FRA. This power was gradually expanded in secret until 1991 when the Government out of fear of a potential public disclosure cancelled these powers ending FRA's access to cable communications. FRA could still intercept communication radio, satellite and microwave relay link which during the 1990s was enough for the needs of FRA. All of this was secret but it all became public in when the Government introduced legislation which was under debate 2007/2008. One of main purposes of the law was to grant the FRA access to cable communications which was perceived as necessary because most international communication went from satellite to fibre-optics. To sun[m]marize, the FRA and its predecessor has been monitoring communication since the late 1930s."

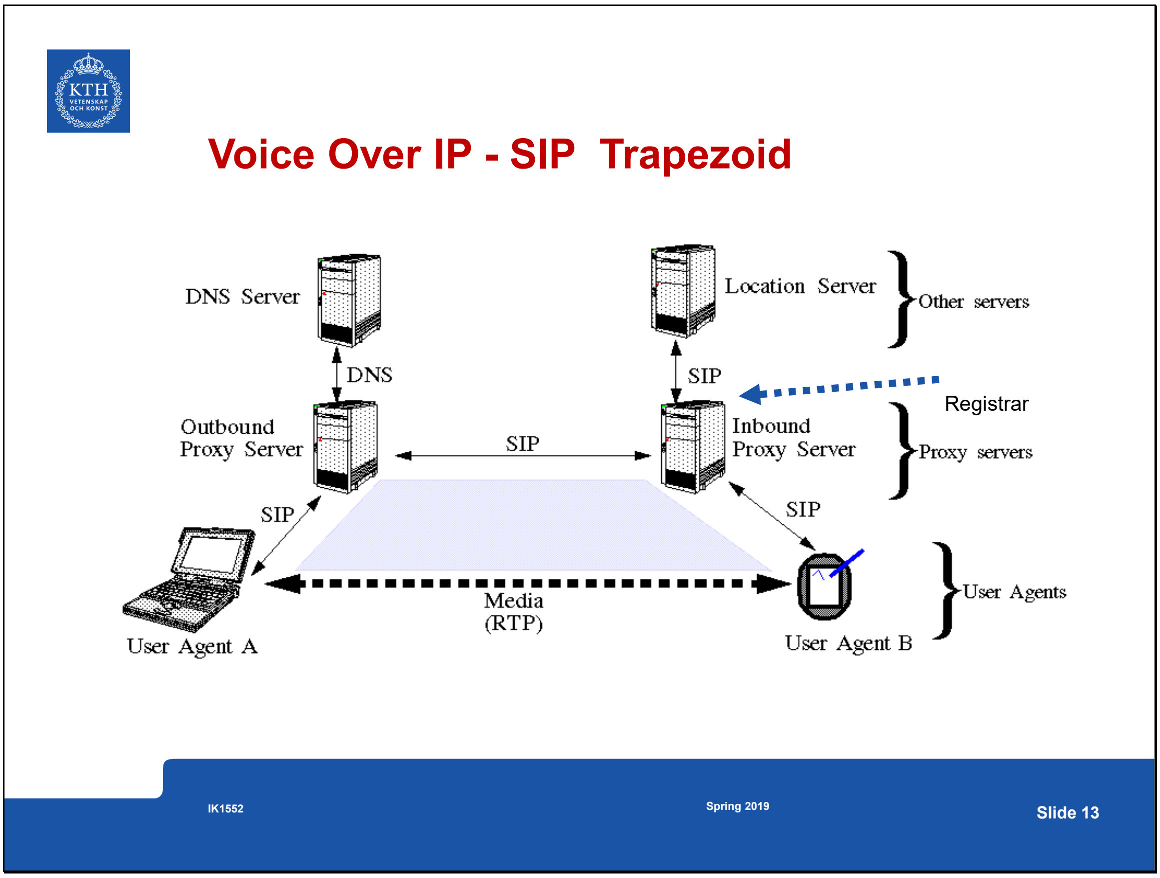
Mark Klamberg, http://klamberg.blogspot.se/search/label/English

See also his presentation "Electronic surveillance and privacy - in light of the Snowden Affair" in Uppsala, September 16th, 2013. Available from http://klamberg.blogspot.se/search/label/English

IK1552 Spring 2019 12

See also his presentation "Electronic surveillance and privacy - in light of the Snowden Affair" in Uppsala, September 16th, 2013. Available from http://klamberg.blogspot.se/search/label/English

Slide 13


Voice Over IP - SIP Trapezoid
DNS Server
Location Server
Other servers
DNS
SIP
Registrar
Outbound
Proxy Server
SIP
Inbound
Proxy Server
Proxy servers
SIP
SIP
User Agents
Media
(RTP)
User Agent A
User Agent B
IK1552
Spring 2019
Slide 13

Slide 14

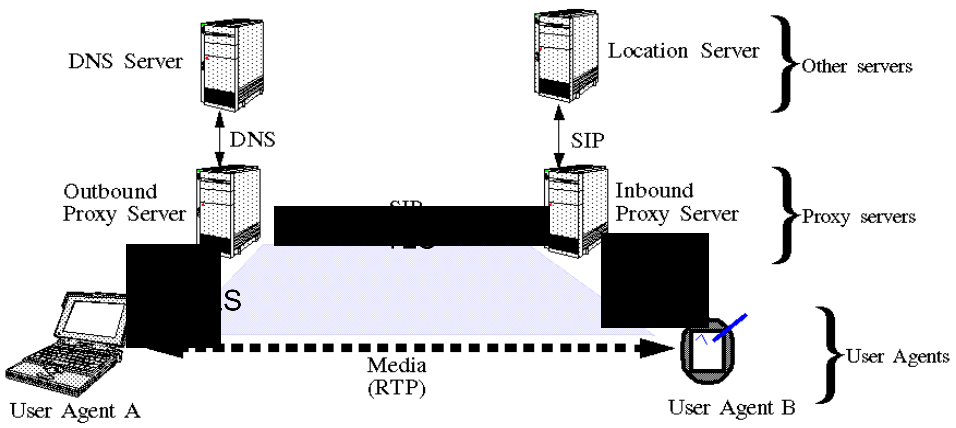
SIP Call setup - Signaling

Ethernet II, Src: 00:0b:db:5c:b1:7d, Dst: 00:00:0c:07:ac:67
Internet Protocol, Src Addr: 130.237.15.248 Dst Addr: 130.237.203.11
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
Session Initiation Protocol
  Request line: INVITE sip:maguire@sip1.it.kth.se;user=phone SIP/2.0
    Method: INVITE
  Message Header
    From: <sip:maguire@it.kth.se;user=phone>;tag=1455337979
    To: <sip:maguire@sip1.it.kth.se;user=phone>
    Call-ID: 58415367@130.237.15.248
    CSeq: 101 INVITE
    Contact: <sip:maguire@130.237.15.248:5060;user=phone;transport=UDP>;expires=1000
    User-Agent: Minisip
    Content-Type: application/sdp
    Via: SIP/2.0/UDP 130.237.15.248:5060;branch=z9hG4bK1587902522
    Content-Length: 533

We can protect this signaling by using TLS or IPsec tunneling; or we can use S/MIME to encrypt the SDP.

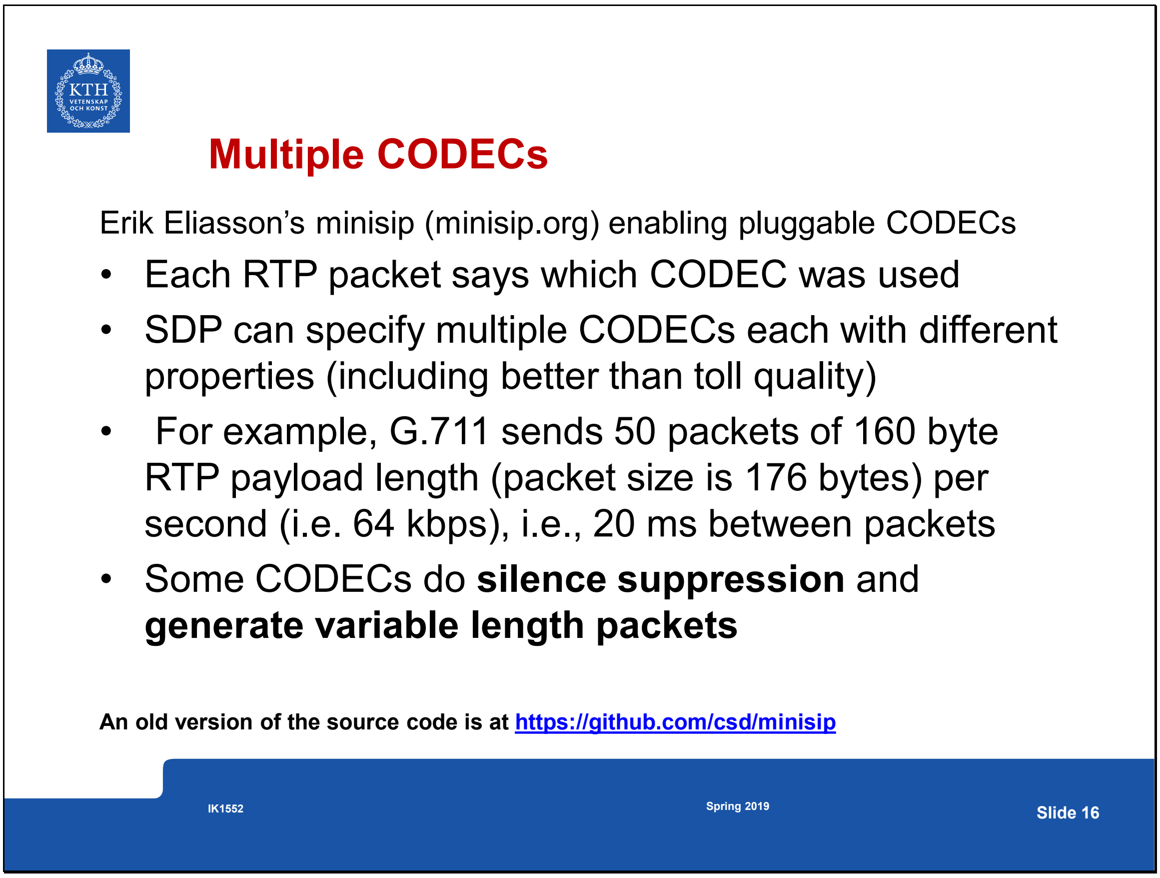
Slide 15

SIP over TLS



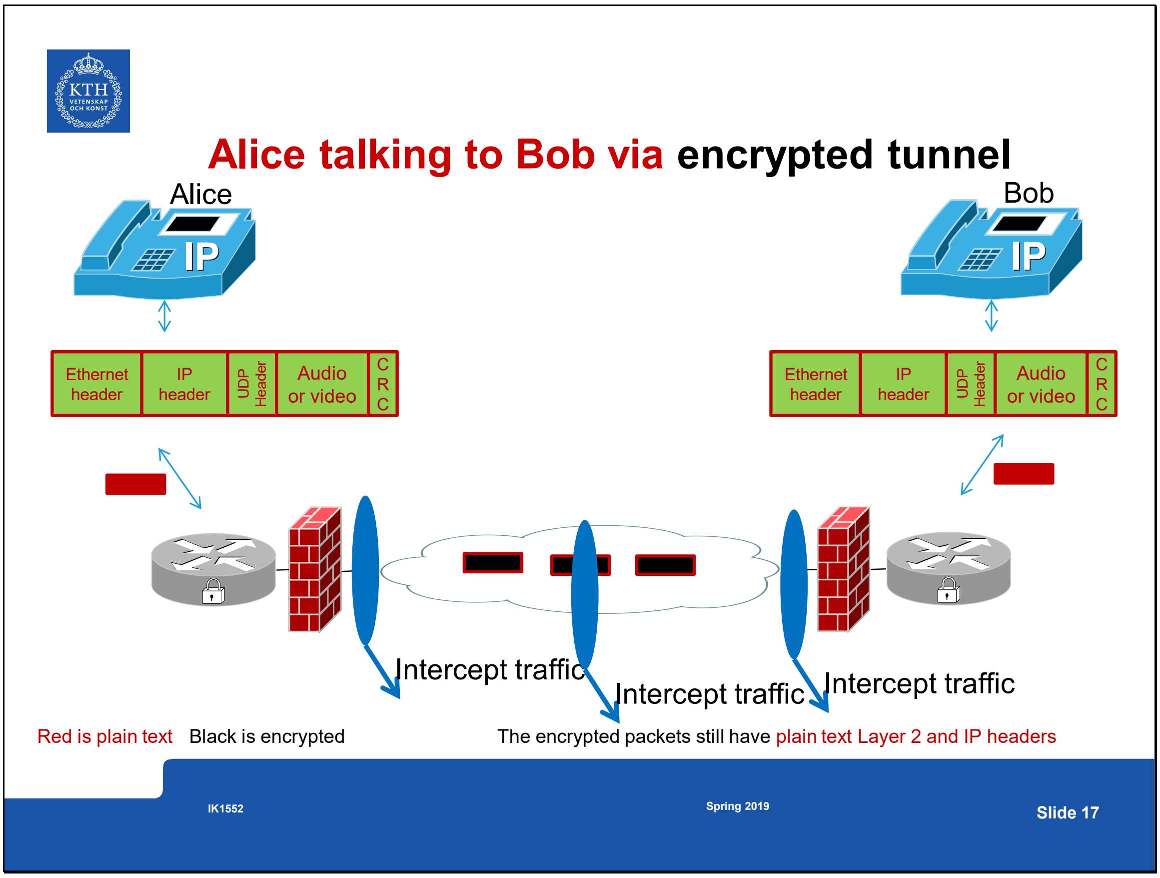
IK1552 Spring 2019 Slide 15

Slide 16

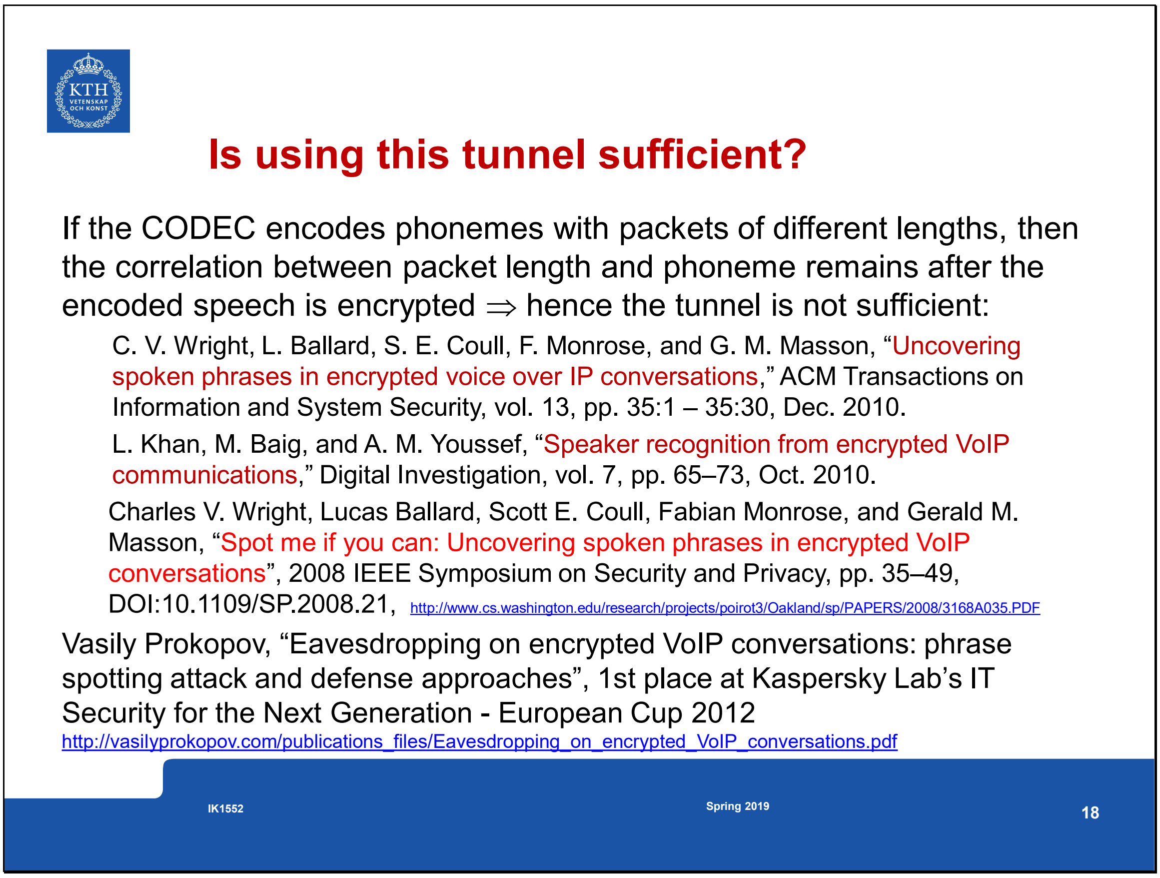


Erik Eliasson, *Secure Internet telephony : design, implementation and performance measurements*, Licentiate thesis. Stockholm, Sweden: KTH Royal Institute of Technology, Electronic, Computer and Software Systems, ECS, 2006, Trita-ICT-ECS AVH-06:04 [Online]. Available: http://urn.kb.se/resolve?urn=urn%3Anbn%3Ase%3Akth%3Adiva-4080

Slide 17

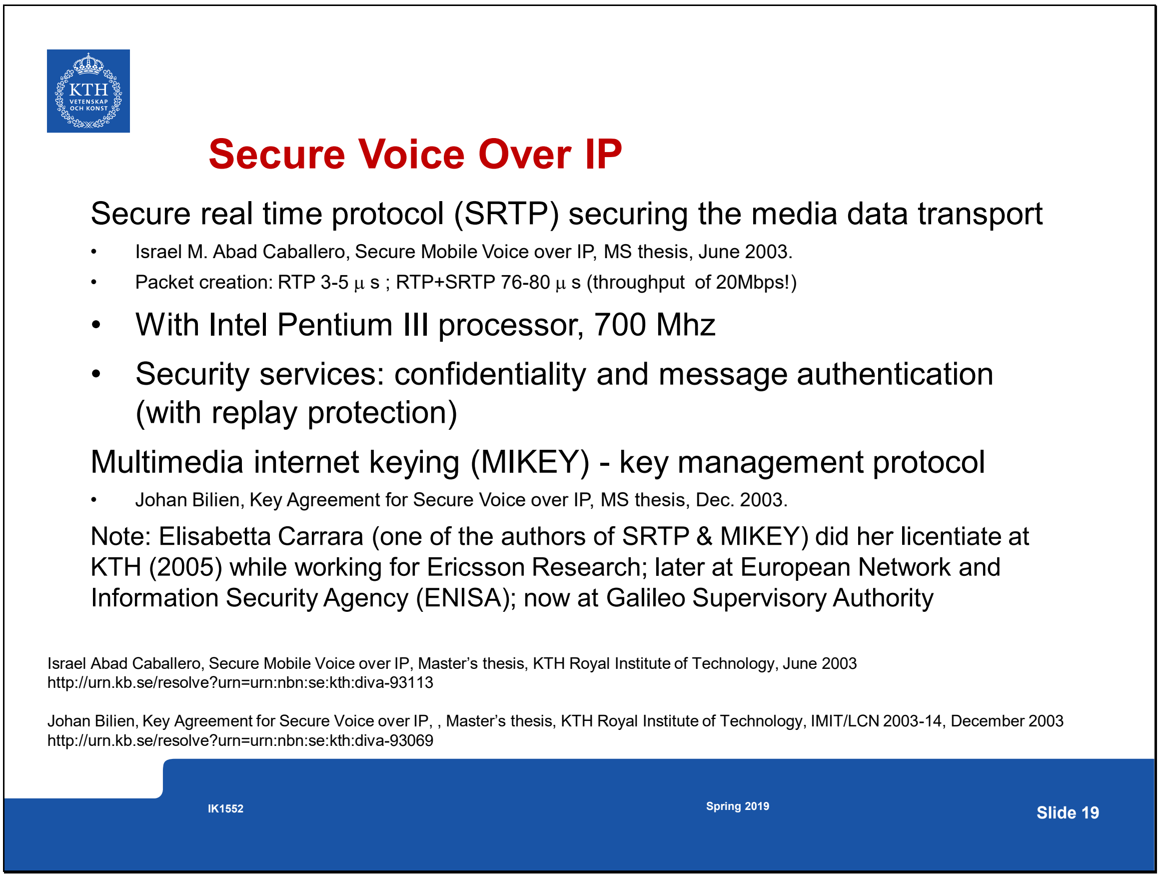

Alice talking to Bob via encrypted tunnel
Alice
Bob
IP
IP
Ethernet header
IP header
UDP Header
Audio or video
CRC
Ethernet header
IP header
UDP Header
Audio or video
CRC
Intercept traffic
Intercept traffic
Intercept traffic
Red is plain text
Black is encrypted
The encrypted packets still have plain text Layer 2 and IP headers
IK1552
Spring 2019
Slide 17

Slide 18



Charles V. Wright, Lucas Ballard, Scott E. Coull, Fabian Monrose, and Gerald M. Masson, "Spot me if you can: Uncovering spoken phrases in encrypted VoIP conversations", 2008 IEEE Symposium on Security and Privacy, pp. 35–49, DOI:10.1109/SP.2008.21, http://www.cs.washington.edu/research/projects/poirot3/Oakland/sp/PAPERS/2008/3168A035.PDF

Slide 19



Israel Abad Caballero, Secure Mobile Voice over IP, Master's thesis, KTH Royal Institute of Technology, June 2003 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-93113

Johan Bilien, Key Agreement for Secure Voice over IP, , Master's thesis, KTH Royal Institute of Technology, IMIT/LCN 2003-14, December 2003 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-93069

Slide 20

SIP Call's SDP

Session Description Protocol

Owner/Creator, Session Id (o): 3344 3344 IN IP4 130.237.15.248

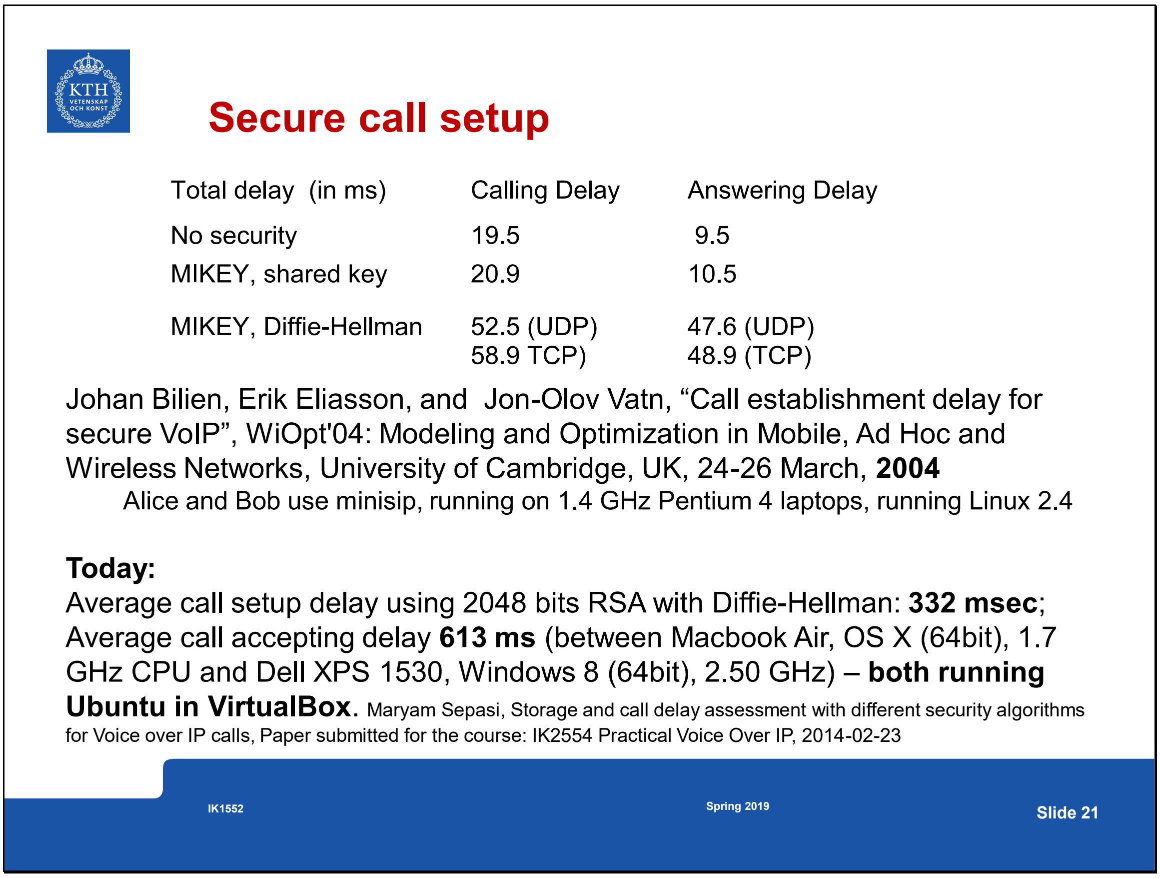
- Session Name (s): Minisip Session
- Connection Information (c): IN IP4 130.237.15.248
- Time Description, active time (t): 0 0
- Media Description, name and address (m): audio 32806 RTP/AVP 0
  - Media Type: audio
  - Media Port: 32806
  - Media Proto: RTP/AVP
  - Media Format: 0
- Media Attribute (a): rtpmap:0 PCMU/8000/1

Media Attribute (a): key-mgmt:mikey

AQAFgH1I7igCAAAcHvouAAAAAAAAAAAAAAAAAAsAxcXV/yACGN4BEGLkPa/2+Z
gTxPxghhHCXQ8AAADEHNGPRiXvhh77qkxq3F1ZkEQUN79OsYpyqlYneR3hdAJtN6
vqY9mDBq0uVNEQKEEvTWiS8eaw7x9CczEsLOnYz4QM0PPyhq1MCrueKHmJ4s7k
DkFxS0F+CPUVehB

IK1552 Spring 2019 Slide 20

Slide 21



Maryam Sepasi, Storage and call delay assessment with different security algorithms for Voice over IP calls, Paper submitted for the course: IK2554 Practical Voice Over IP, 2014-02-23

Slide 22

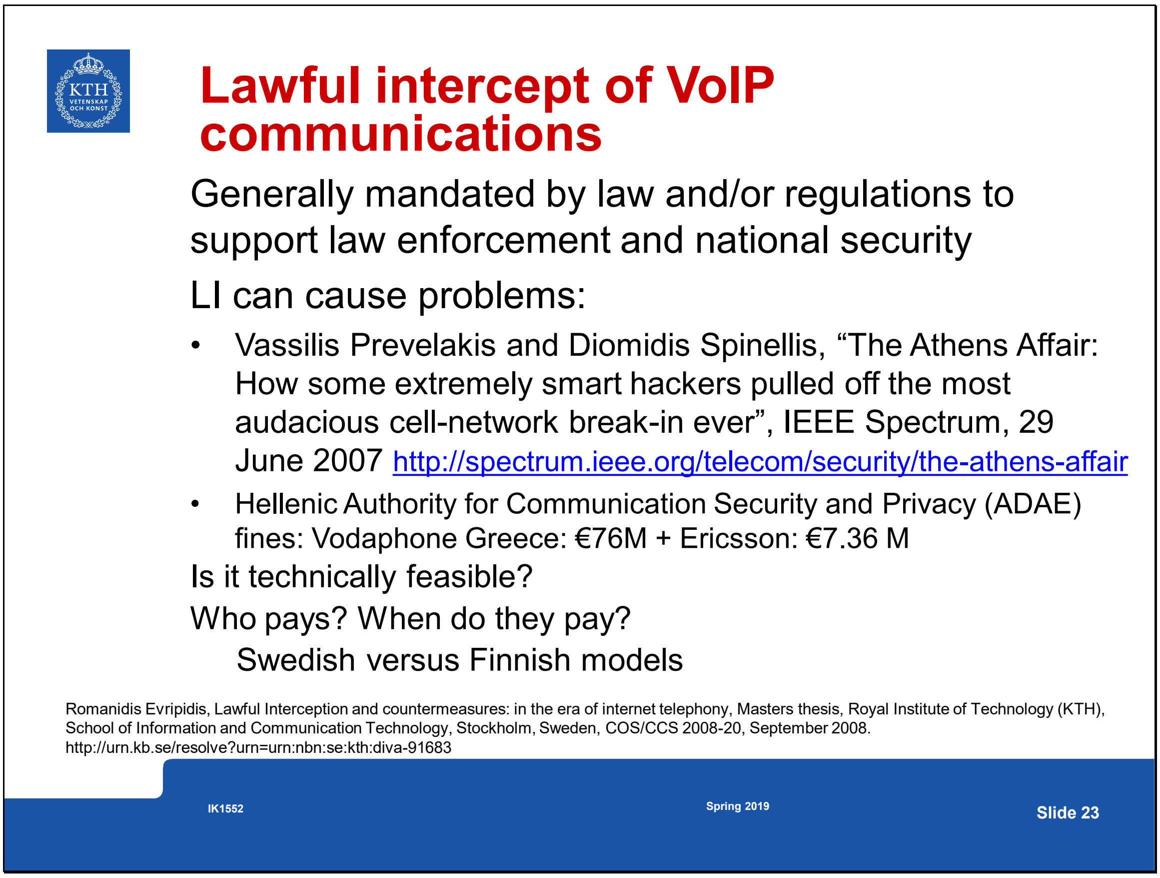
Reasonably Available Information

Operators are only required to provide information to law enforcement **if it is reasonably available**. For example, "call-identifying information is reasonably available to a carrier if it is present at an intercept access point and can be made available without the carrier being unduly burdened with network modifications”

The EU statute is similar in identifying that such information may be required when this is **technically feasible** <u>and</u> **economically feasible**.

- Thus Call Forwarding Information might **not** always be reasonably available in a SIP environment - since the call forwarding could happen outside the control of a given operator.
- Similarily Dialed-Digit Extraction might **not** be available in a SIP environment since the actual IP address of the source and destination might be inside encrypted SDP
- …

Slide 23



Romanidis Evripidis, Lawful Interception and countermeasures: in the era of internet telephony, Masters thesis, Royal Institute of Technology (KTH), School of Information and Communication Technology, Stockholm, Sweden, COS/CCS 2008-20, September 2008. http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-91683

Slide 24

Lawful Intercept and "Pen Traces"

SIP call is setup by communicating with the **user's agent** -- which knows where the user can be contacted

- Potentially you could apply a court order to this agent
- However, the call setup (SDP) could be encrypted with S/MIME so you need this agent's help - but this reveals that you are interested

Furthermore, the actual communication goes **directly** between the parties and it is **encrypted data** - for which the operators of the networks over which it passes over do **not** have the key

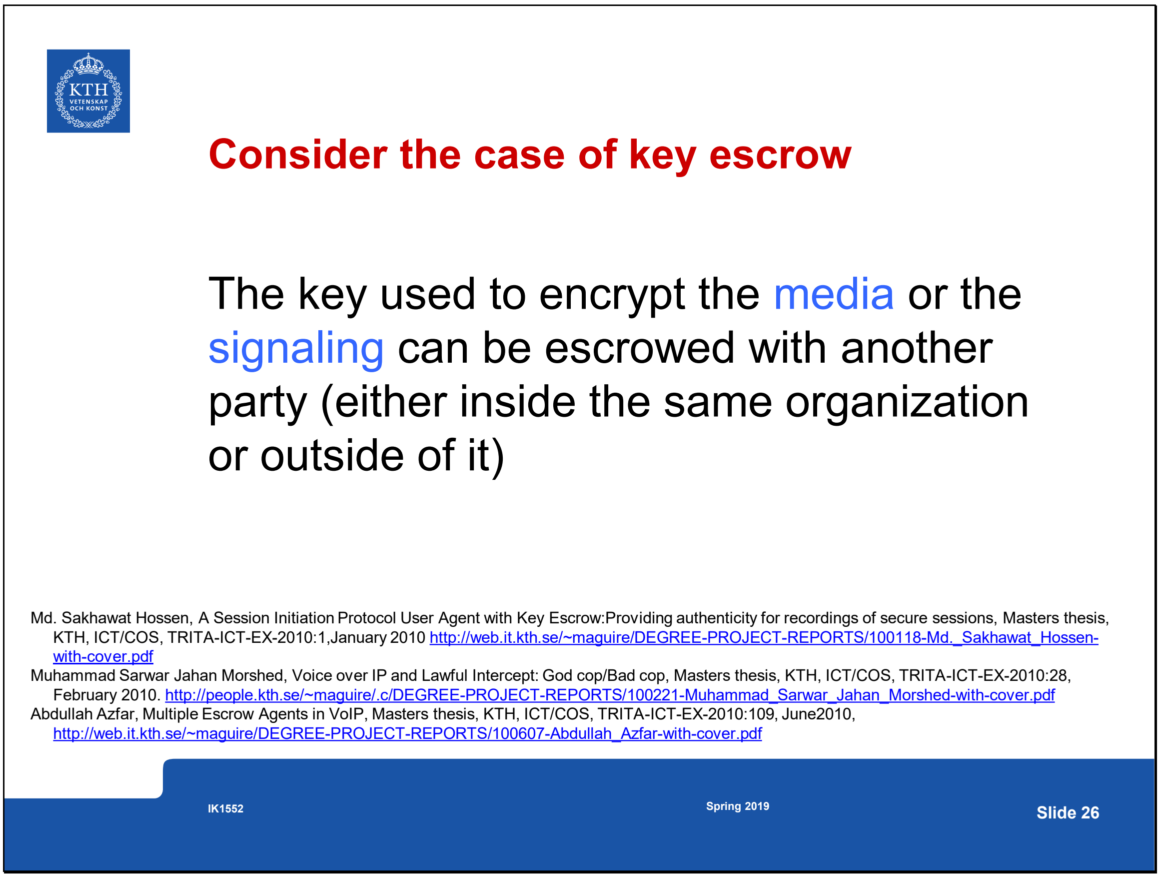
Slide 25

Will VoIP calls have to:

Be stored for **compliance** reasons?
Be stored for **discovery** reasons?
Will they have to be **indexed**? (to make them **accessible**)

UK is proposing that top level ISPs store all records of Internet communications (date, time, sender/ caller, receiver/callee, URL, cell ID, IP address(es), routing, duration, …) to make it *convenient* for the government to access them, because they do not want to have to pay each of the individual ISPs, and to limit the number of parties that they have to deal with. (See EU Data Retention Directive (EUDRD).)

Slide 26

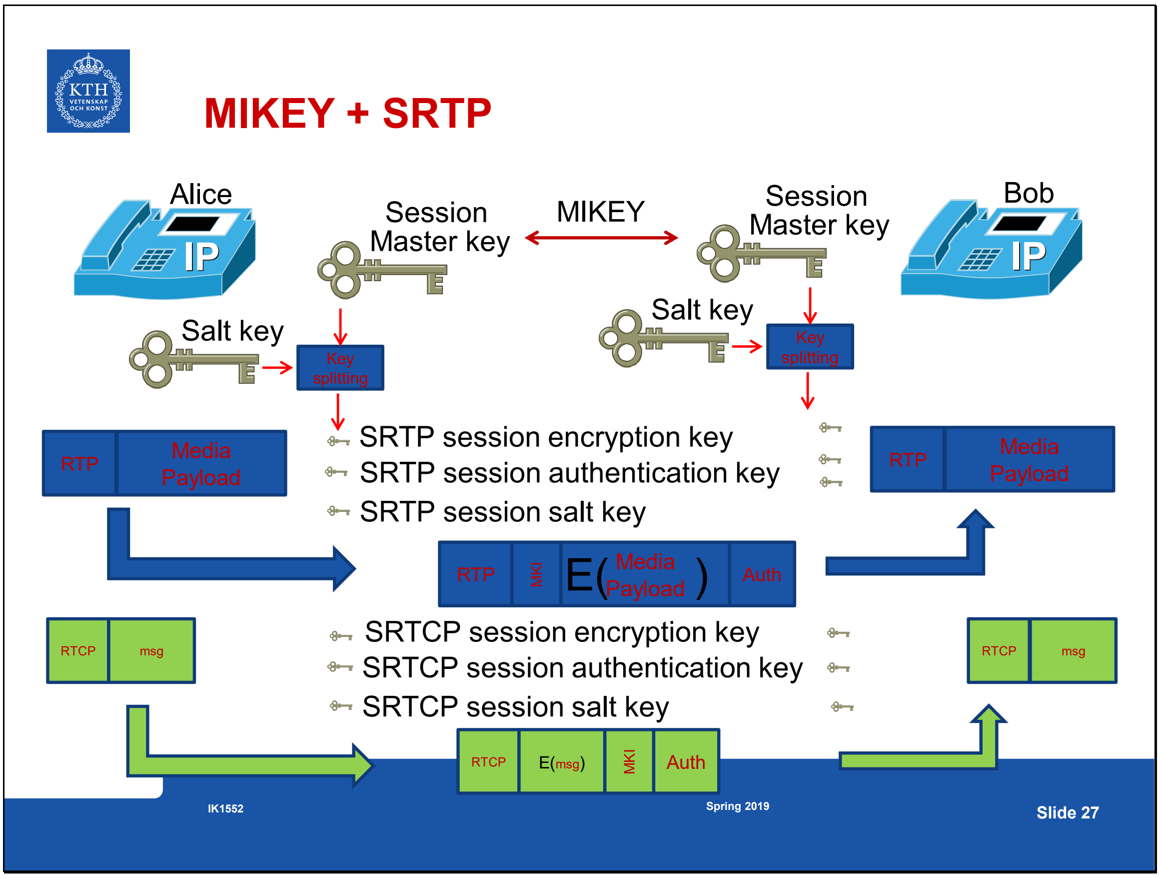


Md. Sakhawat Hossen, A Session Initiation Protocol User Agent with Key Escrow:Providing authenticity for recordings of secure sessions, Masters thesis, KTH, ICT/COS, TRITA-ICT-EX-2010:1,January 2010 http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/100118-Md._Sakhawat_Hossen-with-cover.pdf

Muhammad Sarwar Jahan Morshed, Voice over IP and Lawful Intercept: God cop/Bad cop, Masters thesis, KTH, ICT/COS, TRITA-ICT-EX-2010:28, February 2010.

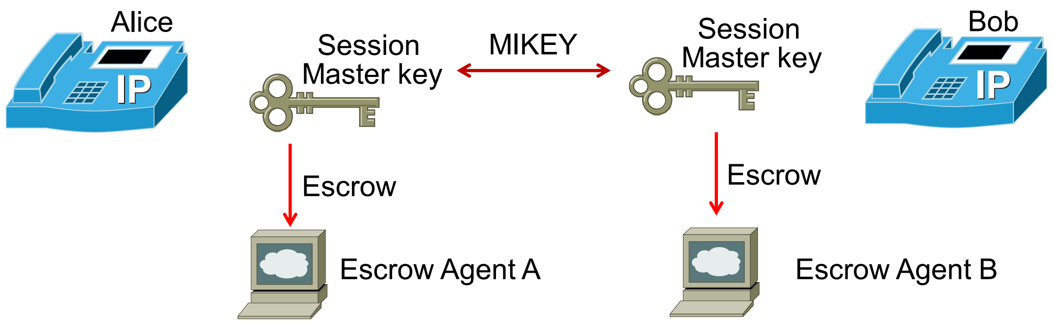
Abdullah Azfar, Multiple Escrow Agents in VoIP, Masters thesis, KTH, ICT/COS, TRITA-ICT-EX-2010:109, June2010, http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/100607-Abdullah_Azfar-with-cover.pdf

Slide 27


MIKEY + SRTP
Alice
Session Master key
MIKEY
Session Master key
Bob
Salt key
Key splitting
Salt key
Key splitting
RTP
Media Payload
SRTP session encryption key
SRTP session authentication key
SRTP session salt key
RTP
Media Payload
RTP
MKI
E(Media Payload)
Auth
RTCP
msg
SRTCP session encryption key
SRTCP session authentication key
SRTCP session salt key
RTCP
msg
RTCP
E(msg)
MKI
Auth
IK1552
Spring 2019
Slide 27

Slide 28

Key Escrow

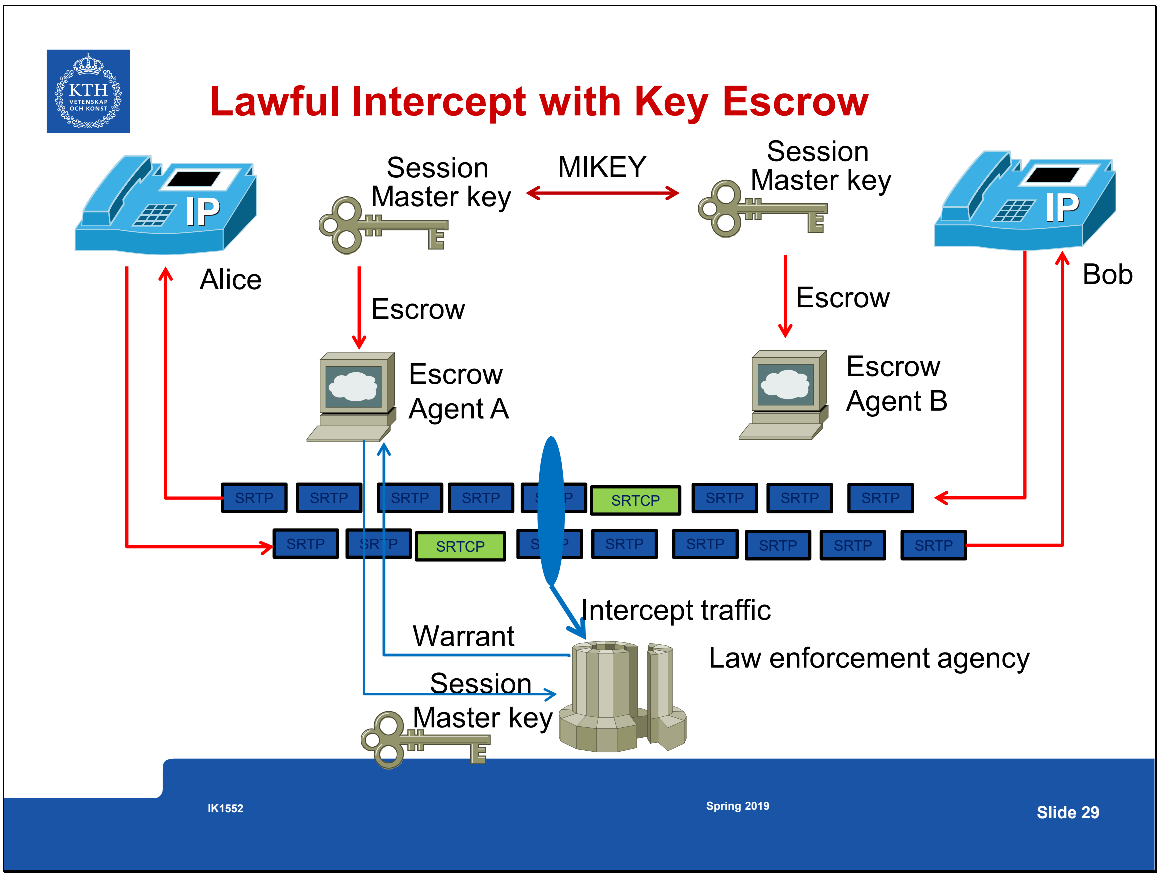


Alice and Bob can independently choose their escrow agent.

Either might choose not to escrow their copy of the session master key – in which case they will not be able to recover the session from a stored copy of the encrypted session - but they might store an unencrypted session.

If an escow agent fails or is unavailable, then the sesssion master key may be unavailable.

Slide 29



Lawful Intercept with Key Escrow
Session Master key
MIKEY
Session Master key
Alice
Bob
Escrow
Escrow
Escrow Agent A
Escrow Agent B
SRTP
SRTCP
Intercept traffic
Warrant
Law enforcement agency
Session Master key
IK1552
Spring 2019
Slide 29

Slide 30

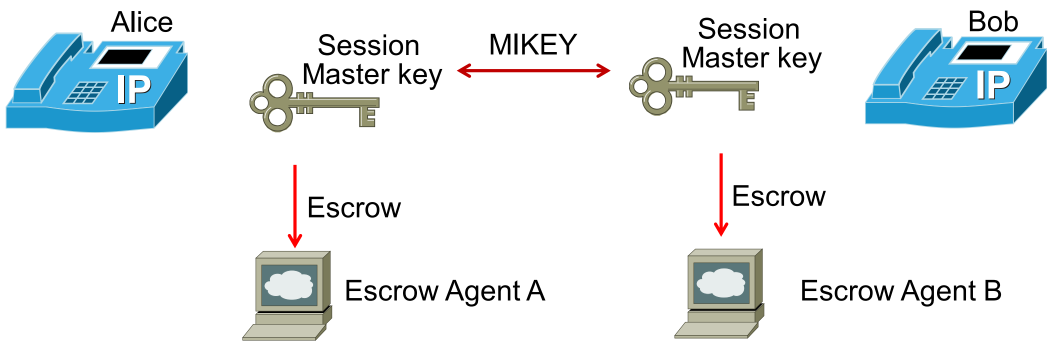
Problems with Lawful Intercept with Key Escrow

Once any one gains access to the session master key they have access to all of the media streams and the control information (contained in the RTCP).

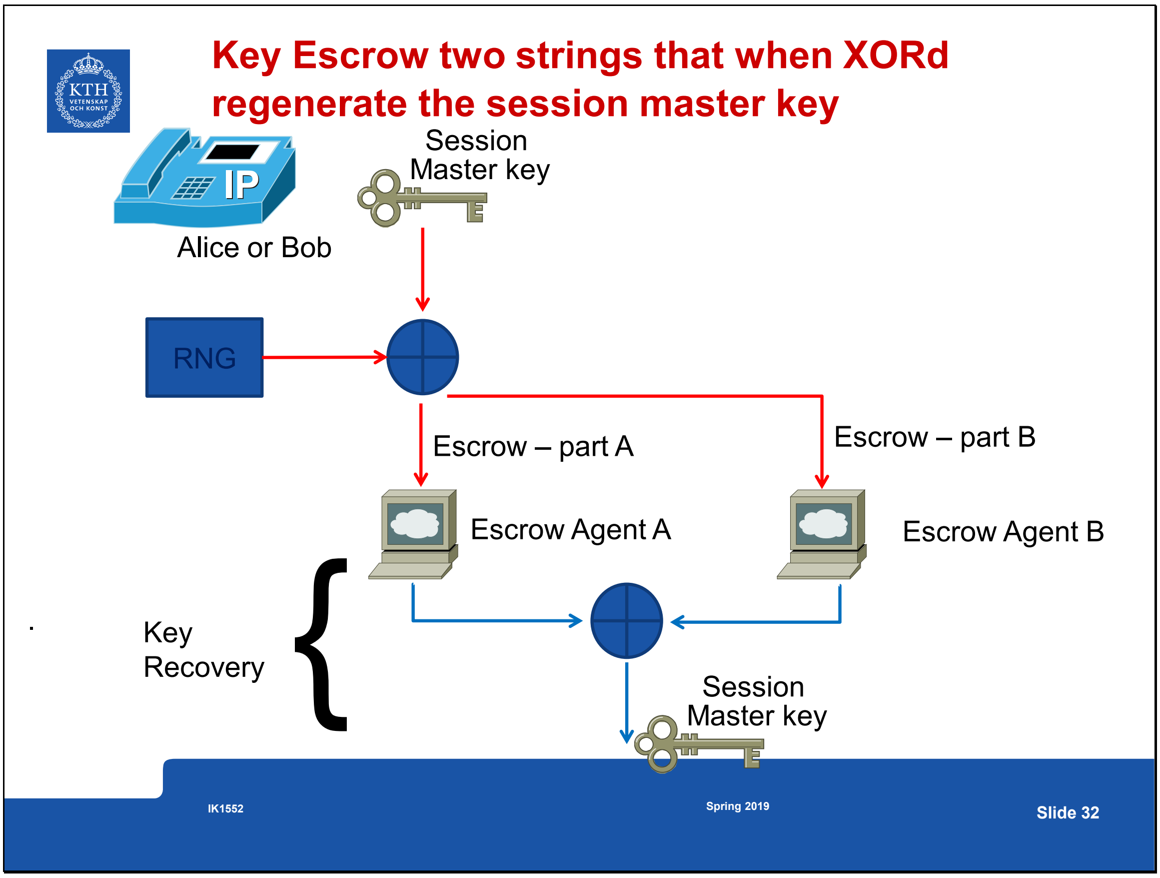
⇒ Given this session master key, a malicious party can fabricate contents of a media stream, create completely ficticous new media stream(s), fabricate control messages, etc.

Slide 31

Key Escrow - revisited

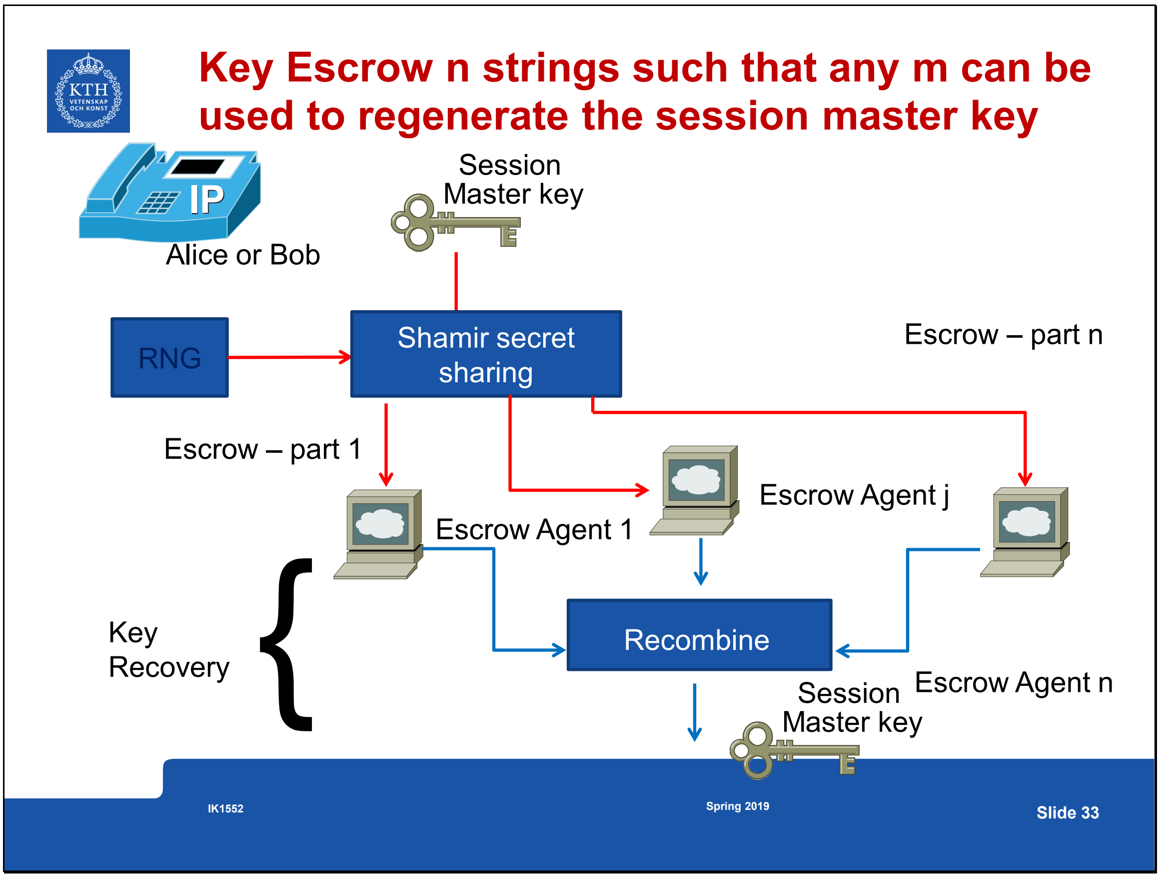


Slide 32



Key Escrow two strings that when XORd regenerate the session master key
Session Master key
IP
Alice or Bob
RNG
Escrow – part A
Escrow – part B
Escrow Agent A
Escrow Agent B
Key Recovery
Session Master key
IK1552
Spring 2019
Slide 32

Slide 33


Key Escrow n strings such that any m can be used to regenerate the session master key
IP
Alice or Bob
Session
Master key
RNG
Shamir secret sharing
Escrow – part n
Escrow – part 1
Escrow Agent j
Escrow Agent 1
Key
Recovery
Recombine
Session
Master key
Escrow Agent n
IK1552
Spring 2019
Slide 33

Slide 34

Evaluation of Key Escrow n of m

A user agent need only wait for n of the m keys to be escrowed – the rest can be escrowed in the background at a later time.

Key recovery can be done despite m-n escrow agents failing or being unavailable.

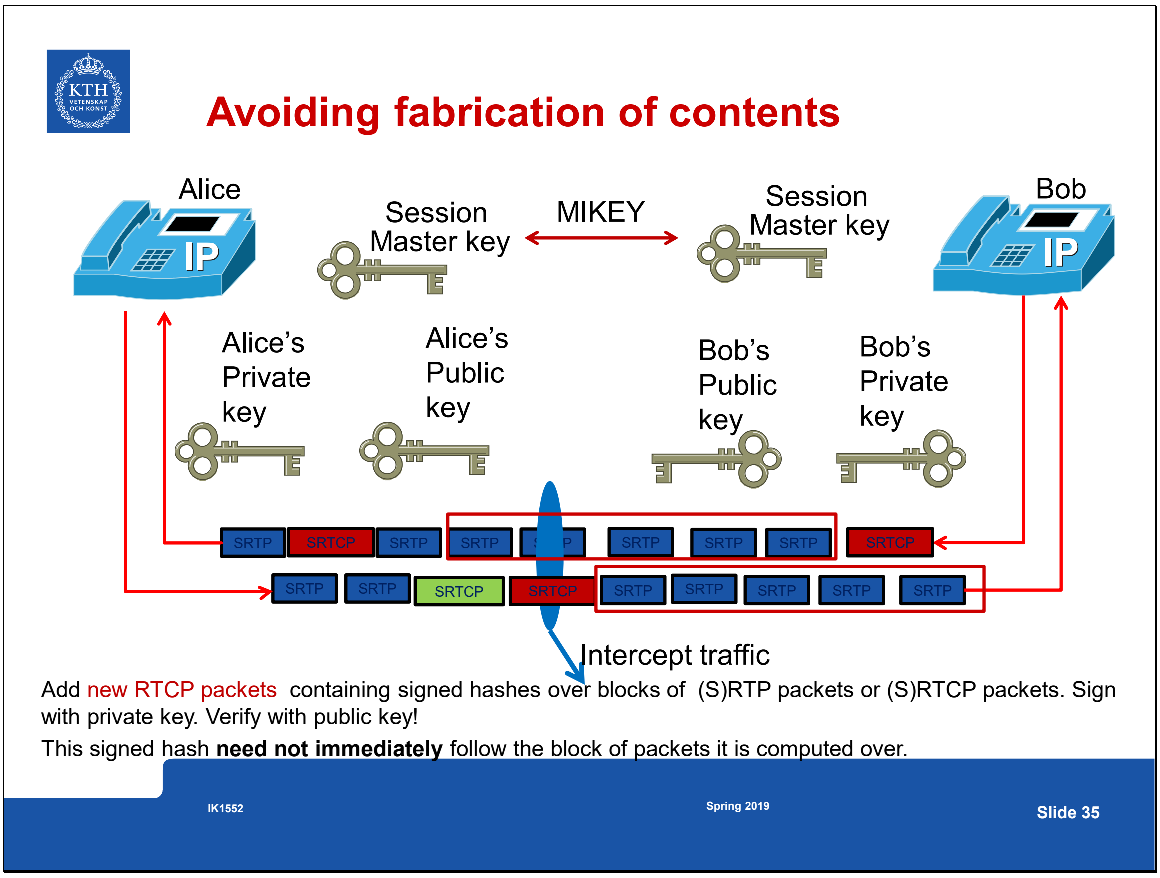
Key recovery can be done as soon as n escrow agents have answered.

Abdullah Azfar, Multiple Escrow Agents in VoIP, Master's thesis, KTH Royal Institute of Technology, TRITA-ICT-EX-2010:109, June 2010
http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-91102

IK1552 Spring 2019 Slide 34

Abdullah Azfar, Multiple Escrow Agents in VoIP, Master's thesis, KTH Royal Institute of Technology, TRITA-ICT-EX-2010:109, June 2010
http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-91102

Slide 35



Md. Sakhawat Hossen A Session Initiation Protocol User Agent with Key Escrow: Providing authenticity for recordings of secure sessions, Master's thesis, KTH Royal Institute of Technology, TRITA-ICT-EX-2010:1, January 2010 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-12143

Muhammad Sarwar Jahan Morshed, Voice over IP and Lawful Intercept: God cop/Bad cop, Master's thesis, KTH Royal Institute of Technology, TRITA-ICT-EX-2010:28, February 2010 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-24260

Slide 36

Avoiding fabrication of contents

Sign blocks of the encrypted call session

⇒ The parties to the call can prove which content is or is not part of their call

⇒ There is no need to make the signing key public, only the corresponding public key is needed – this could be published in a public place/record for later use.

This potentially leaks private key bits due to the large number of signatures! However, it is not clear what rate this leakage occurs at (especially with video conferencing).

Slide 37

Strict source routing

Explicitly routing a packet along a set of IP addresses, each forwards the packet after removing its own address

Slide 38

Onion Routing

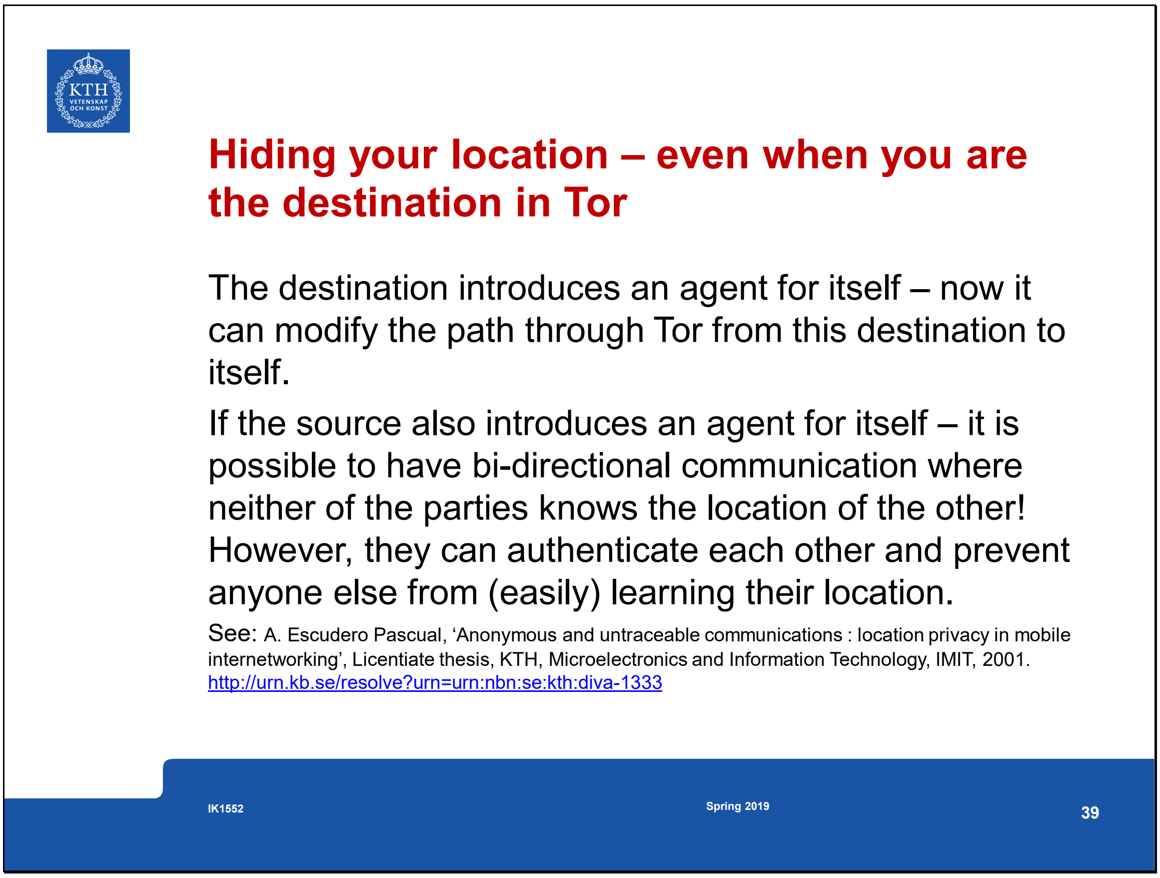
Logically: To send a message the sender computes a path through the network, then repeatedly moves each hop's addressing information (starting with the final destination) into an encrypted envelop and encrypts this header with the public key of the router that forwards it for the next hop):

$E\_header_{first\_hop}$ (E_header_{d-l} … (E_header_{d-2} (E_header_{d-1} E_message)) …)

- Each router forwards the packet after removing its own address and decrypting the header with the destination address of the next hop (this header was encrypted with its public key – hence it uses it own private key for decryption).
- Each router only decrypts what it receive and learns only the next hop destination

One version of this is Tor which uses a series of relays: https://www.torproject.org/

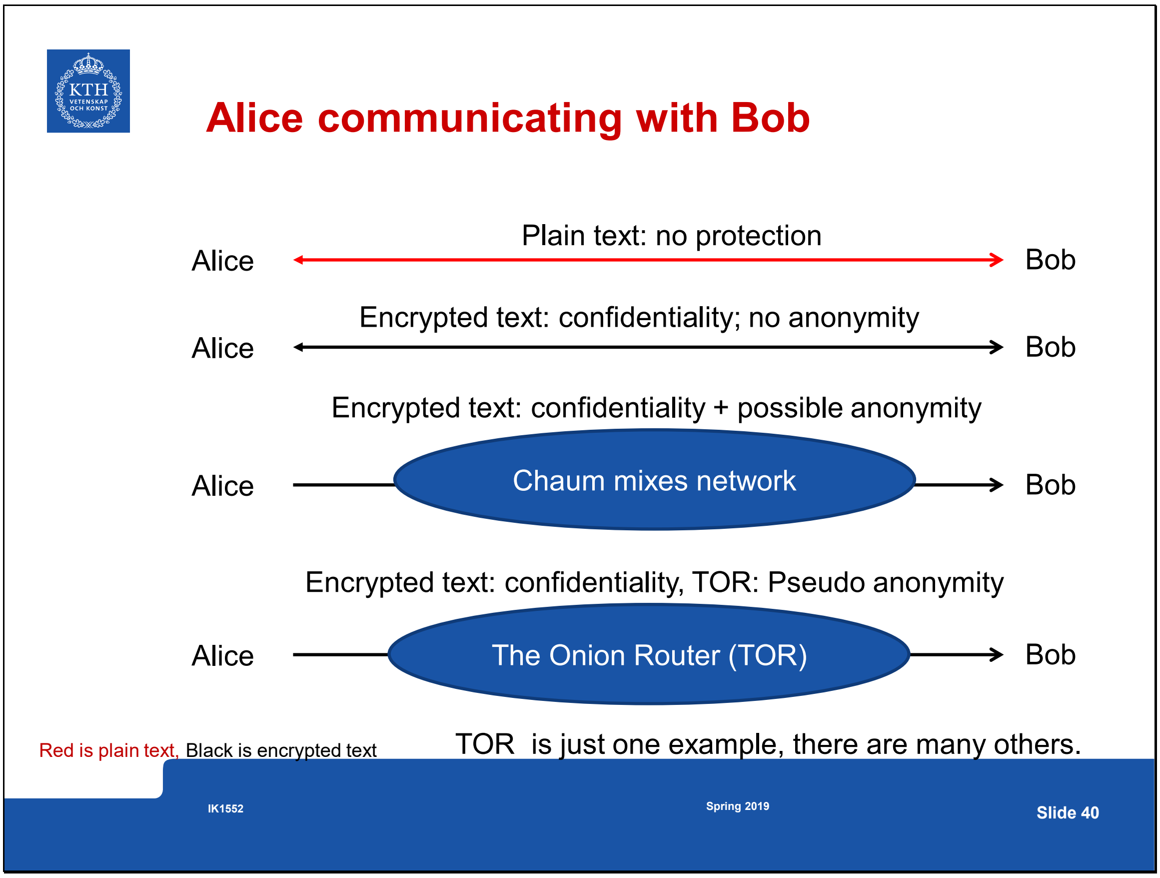
Slide 39



A. Escudero Pascual, 'Anonymous and untraceable communications : location privacy in mobile internetworking', Licentiate thesis, KTH, Microelectronics and Information Technology, IMIT, 2001. http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-1333

A. Escudero-Pascual and G. Q. Maguire Jr., 'Role(s) of a proxy in location based services', in 13TH IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Vol. 1-5, Proceedings: Sailing the waves of the Wireless Ocean, 2002, pp. 1252–1256, doi: 10.1109/PIMRC.2002.1045229

Slide 40


Alice communicating with Bob
Plain text: no protection
Alice
Bob
Encrypted text: confidentiality; no anonymity
Alice
Bob
Encrypted text: confidentiality + possible anonymity
Alice
Chaum mixes network
Bob
Encrypted text: confidentiality, TOR: Pseudo anonymity
Alice
The Onion Router (TOR)
Bob
Red is plain text, Black is encrypted text
TOR is just one example, there are many others.
IK1552
Spring 2019
Slide 40

Slide 41

Traffic analysis & spotting

X. Wang, D. S. Reeves, and S. F. Wu, 'Inter-Packet Delay Based Correlation for Tracing Encrypted Connections Through Stepping Stones', in *Proceedings of the 7th European Symposium on Research in Computer Security*, London, UK, UK, 2002, pp. 244–263, Available at http://dl.acm.org/citation.cfm?id=646649.699363.

Y. J. Pyun, Y. Park, D. S. Reeves, X. Wang, and P. Ning, 'Interval-based flow watermarking for tracing interactive traffic', *Computer Networks*, 56 (5):1646–1665, March 2012, DOI:10.1016/j.comnet.2012.01.017.

Scott E. Coull, "Traffic Analysis", In H. van Tilborg and S. Jajodia (Eds.) Encyclopedia of Cryptography and Security (2nd Edition). Springer Publishing. 2011. pp.1311 - 1313. http://www.scottcoull.com/Traffic_Analysis.pdf

Leaking anonymity:

John Geddes, Rob Jansen, and Nicholas Hopper. "How Low Can You Go: Balancing Performance with Anonymity in Tor" at PETS 2013 http://www-users.cs.umn.edu/~hopper/howlow-pets2013.pdf

Nicholas Hopper, Eugene Y. Vasserman, and Eric Chan-Tin. "How much anonymity does network latency leak?" ACM Transactions on Information and System Security (TISSEC), 13(2):1-28, February 2010. http://www-users.cs.umn.edu/~hopper/tissec-latency-leak.pdf

Zi Lin and Nicholas Hopper. "New Attacks on Timing-based Network Flow Watermarks" at USENIX Security 2012. http://www-users.cs.umn.edu/~hopper/flow-wm-sec12.pdf

IK1552 Spring 2019 41

X. Wang and D. S. Reeves, 'Robust correlation of encrypted attack traffic through stepping stones by manipulation of interpacket delays', CCS '03 Proceedings of the 10th ACM conference on Computer and communications security, 2003, pp. 20-29, DOI:10.1145/948109.948115, Available at http://portal.acm.org/citation.cfm?doid=948109.948115.

P. Peng, P. Ning, D. S. Reeves, and X. Wang, 'Active Timing-Based Correlation of Perturbed Traffic Flows with Chaff Packets', in Proceedings of the Second International Workshop on Security in Distributed Computing Systems (SDCS) (ICDCSW'05) - Volume 02, Washington, DC, USA, 2005, pp. 107–113, DOI:10.1109/ICDCSW.2005.30, Available at http://dx.doi.org/10.1109/ICDCSW.2005.30

Young June Pyun, Young Hee Park, Douglas S. Reeves, Xinyuan Wang and Peng Ning. Interval-based Flow Watermarking for Tracing Interactive Traffic. In Computer Networks Journal, 56(5):1646-1665, March 2012. and other papers at: http://cs.gmu.edu/~xwangc/

Charles V. Wright, Fabian Monrose, and Gerald M. Masson, "Towards better protocol identification using profile HMMs", JHU Technical Report JHU-SPAR051201, http://www.cs.jhu.edu/~cwright/hmm-techreport.pdf

Charles V. Wright, Fabian Monrose, and Gerald M. Masson, "On Inferring Application Protocol Behaviors in Encrypted Network Traffic", JHU Technical Report JHU-SPAR060315, http://www.cs.jhu.edu/~cwright/hmm-techreport2.pdf

T. He, P. Venkitasubramaniam, and L. Tong, ‘Packet Scheduling Against Stepping-stone Attacks with Chaff’, in Proceedings of the 2006 IEEE Conference on Military Communications, Piscataway, NJ, USA, 2006, pp. 356–362, Available at http://dl.acm.org/citation.cfm?id=1896579.1896634

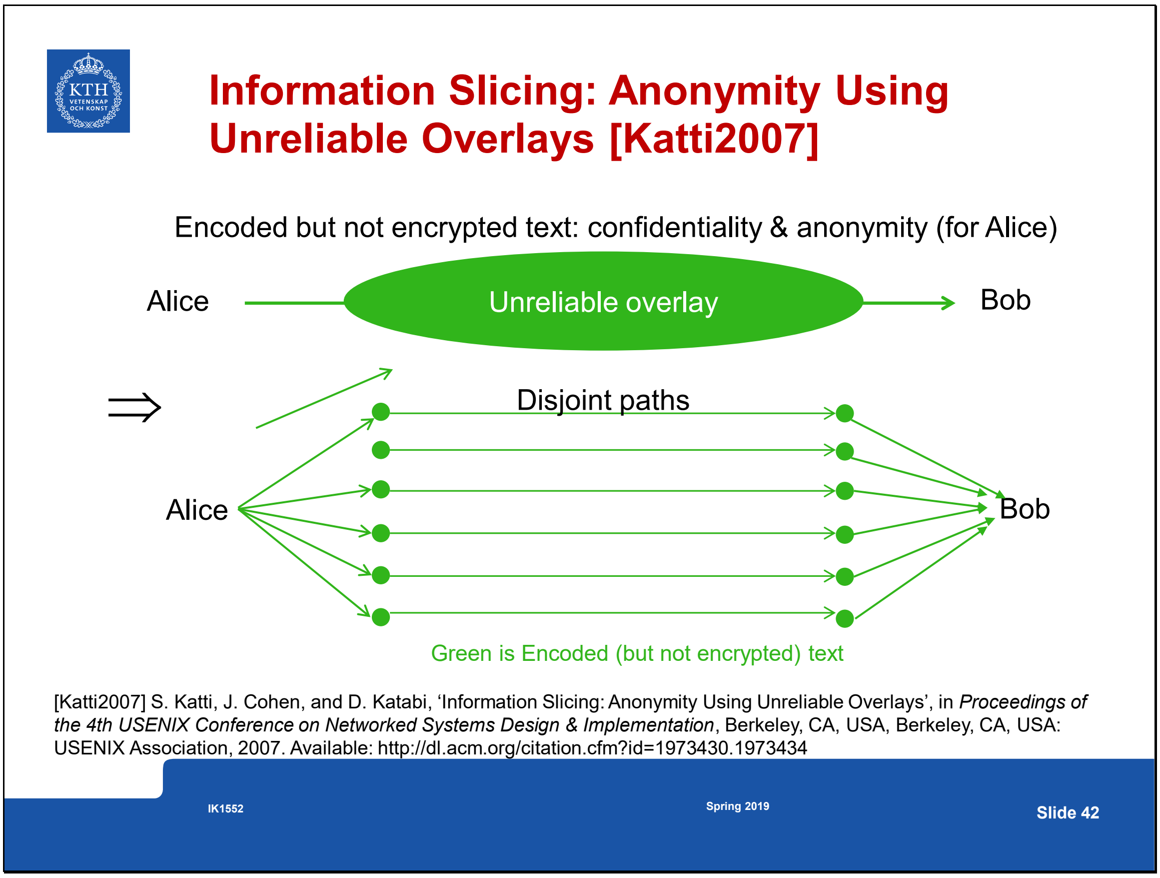
T. He and L. Tong, ‘Detecting Information Flows: Improving Chaff Tolerance by Joint Detection’, presented at the 41st Annual Conference on Information Sciences and Systems, 2007. CISS ’07., 2007, pp. 51–56, DOI:10.1109/CISS.2007.4298272, Available at http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4298272.

John Geddes, Rob Jansen, and Nicholas Hopper. "How Low Can You Go: Balancing Performance with Anonymity in Tor <http://www-users.cs.umn.edu/%7Ehopper/howlow-pets2013.pdf>," at PETS 2013 http://www-users.cs.umn.edu/~hopper/howlow-pets2013.pdf

Nicholas Hopper, Eugene Y. Vasserman, and Eric Chan-Tin. "How much anonymity does network latency leak? <http://www-users.cs.umn.edu/%7Ehopper/tissec-latency-leak.pdf>" ACM Transactions on Information and System Security (TISSEC), 13(2):1-28, February 2010. http://www-users.cs.umn.edu/~hopper/tissec-latency-leak.pdf

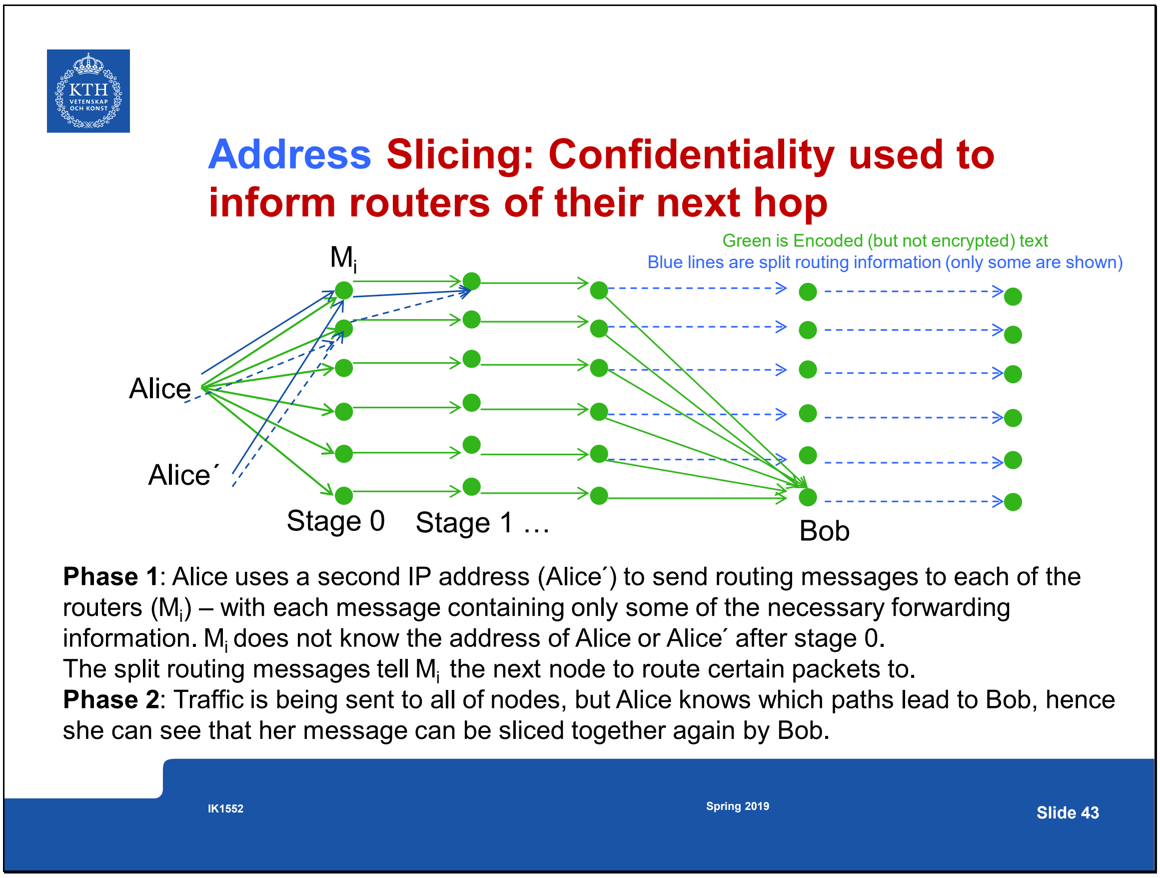
Zi Lin and Nicholas Hopper. "New Attacks on Timing-based Network Flow Watermarks <http://www-users.cs.umn.edu/%7Ehopper/flow-wm-sec12.pdf>," at USENIX Security 2012. http://www-users.cs.umn.edu/~hopper/flow-wm-sec12.pdf

Slide 42



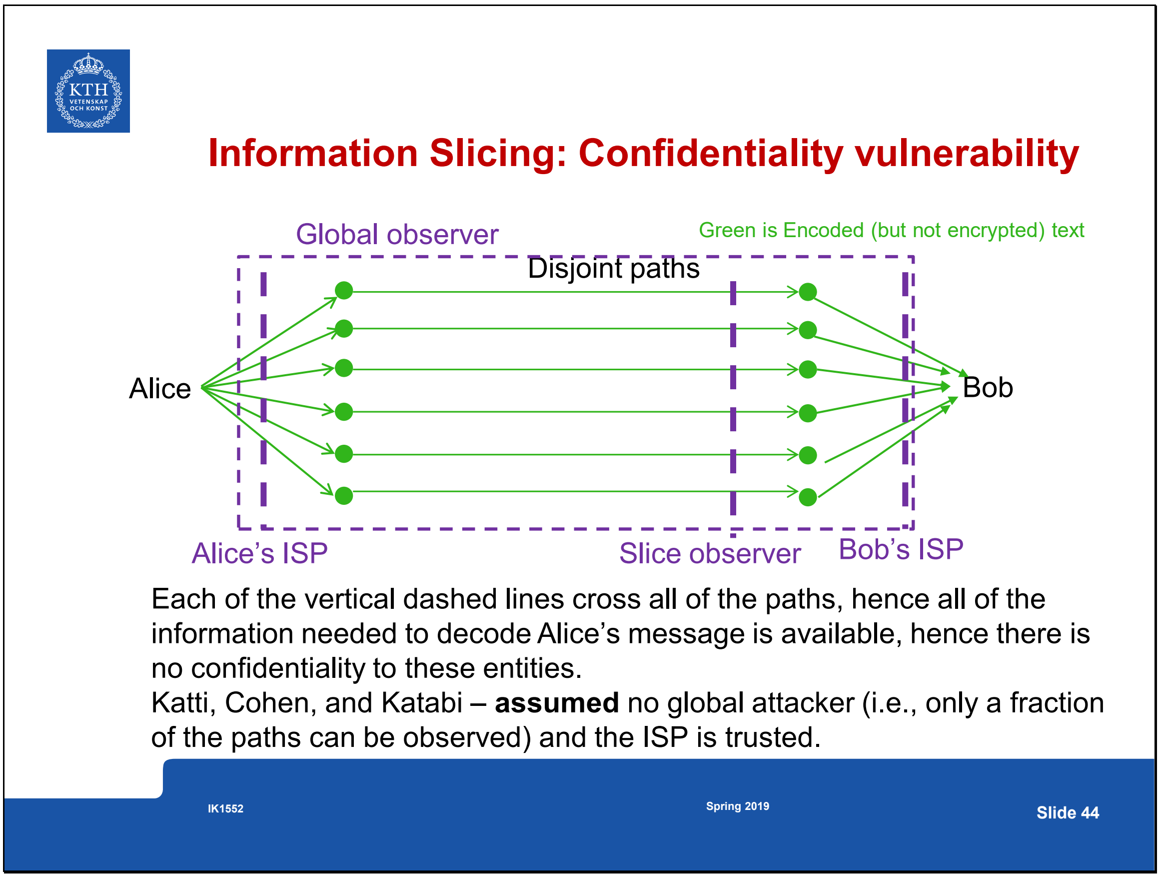
[Katti2007] S. Katti, J. Cohen, and D. Katabi, 'Information Slicing: Anonymity Using Unreliable Overlays', in *Proceedings of the 4th USENIX Conference on Networked Systems Design & Implementation*, Berkeley, CA, USA, Berkeley, CA, USA: USENIX Association, 2007, pp. 4–4 [Online]. Available: http://dl.acm.org/citation.cfm?id=1973430.1973434

Slide 43



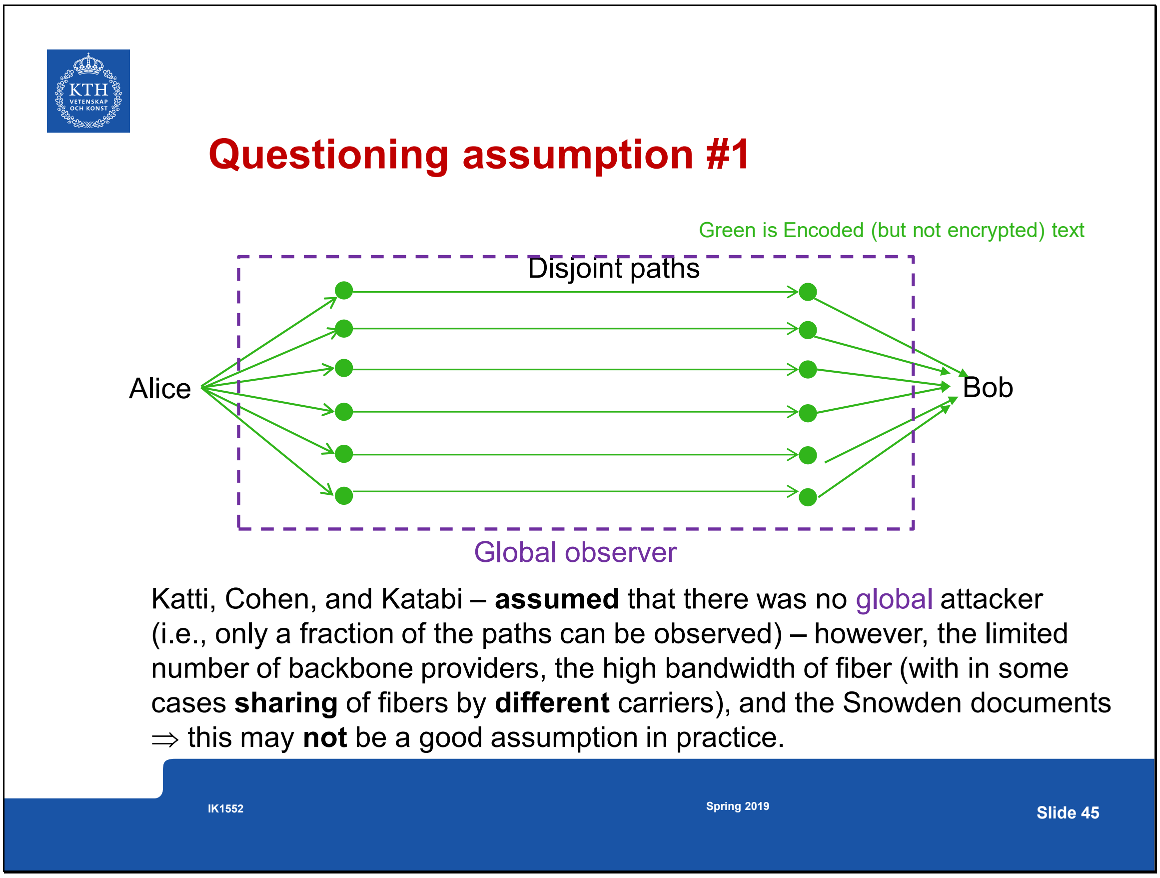
[Katti2007] S. Katti, J. Cohen, and D. Katabi, ‘Information Slicing: Anonymity Using Unreliable Overlays’, in *Proceedings of the 4th USENIX Conference on Networked Systems Design & Implementation*, Berkeley, CA, USA, Berkeley, CA, USA: USENIX Association, 2007, pp. 4–4 [Online]. Available: http://dl.acm.org/citation.cfm?id=1973430.1973434

Slide 44



[Katti2007] S. Katti, J. Cohen, and D. Katabi, 'Information Slicing: Anonymity Using Unreliable Overlays', in *Proceedings of the 4th USENIX Conference on Networked Systems Design & Implementation*, Berkeley, CA, USA, Berkeley, CA, USA: USENIX Association, 2007, pp. 4–4 [Online]. Available: http://dl.acm.org/citation.cfm?id=1973430.1973434

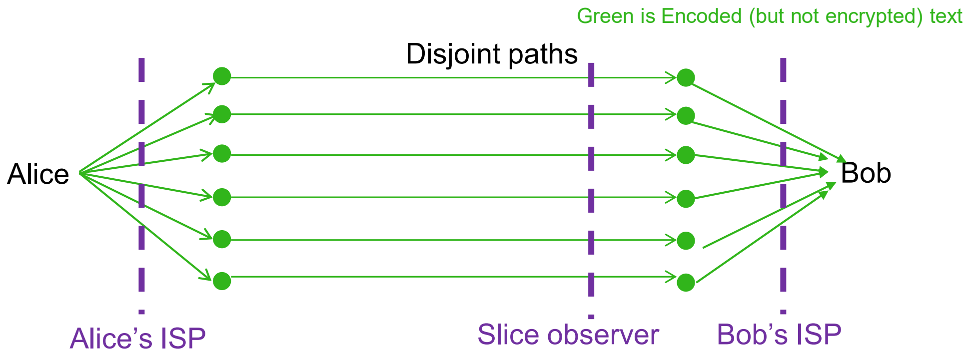
Slide 45



[Katti2007] S. Katti, J. Cohen, and D. Katabi, 'Information Slicing: Anonymity Using Unreliable Overlays', in *Proceedings of the 4th USENIX Conference on Networked Systems Design & Implementation*, Berkeley, CA, USA, Berkeley, CA, USA: USENIX Association, 2007, pp. 4–4 [Online]. Available: http://dl.acm.org/citation.cfm?id=1973430.1973434

Slide 46

Questioning assumption #2



Katti, Cohen, and Katabi – **assumed** that each end user's ISP is trusted – however, the limited number of ISPs and the existence of lawful intercept requirements (by the local governments) ⇒ this may **not** be a good assumption in practice.

In some cases a slice observer may also be feasible.

[Katti2007] S. Katti, J. Cohen, and D. Katabi, 'Information Slicing: Anonymity Using Unreliable Overlays', in *Proceedings of the 4th USENIX Conference on Networked Systems Design & Implementation*, Berkeley, CA, USA, Berkeley, CA, USA: USENIX Association, 2007, pp. 4–4 [Online]. Available: http://dl.acm.org/citation.cfm?id=1973430.1973434

Jaya Baloo, Lawful Interception of IP Lawful Interception of IP Traffic, Draft 1, Black Hat Europe 2003, May 2003
http://www.blackhat.com/presentations/bh-europe-03/bh-europe-03-baloo.pdf

ETSI TS 101 331, Telecommunications security; Lawful Interception (LI); Requirements of law enforcement agencies, V1.1.1, August 2001.

ETSI TS 33.108 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Handover Interface for Lawful Interception, V5.1.0, September 2002.

Global LI Industry Forum, Inc. *http://www.gliif.org/*

See also:

Communications Assistance for Law Enforcement Act. CALEA - 47 USC 1001-1010. Title 47--Telegraphs, Telephones, and Radiotelegraphs. Chapter 9--Interception of Digital and Other

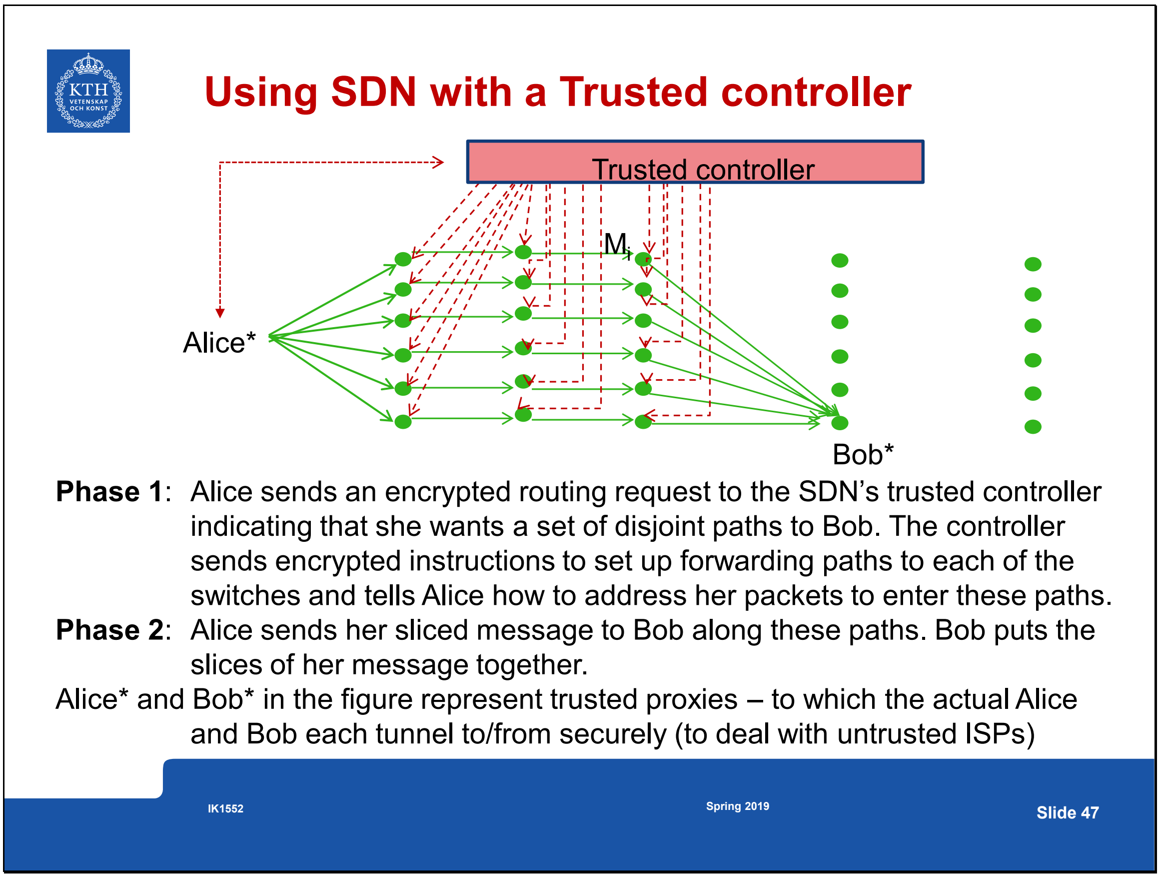
Communications
http://www.techlawjournal.com/agencies/calea/47usc1001.htm

Matt Holdrege, “Supporting Lawful Intercept in IP-based Networks”, IEEE Homeland Defense Series, March 2002
http://www.ewh.ieee.org/r6/lac/csspsvts/briefings/holdrege.pdf

United States Department of Justice, Federal Bureau of Investigation and Drug Enforcement Administration, Joint Petition [to US FCC] for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, 10 March, 2004
http://www.steptoe.com/publications/FBI_Petition_for_Rulemaking_on_CALEA.pdf

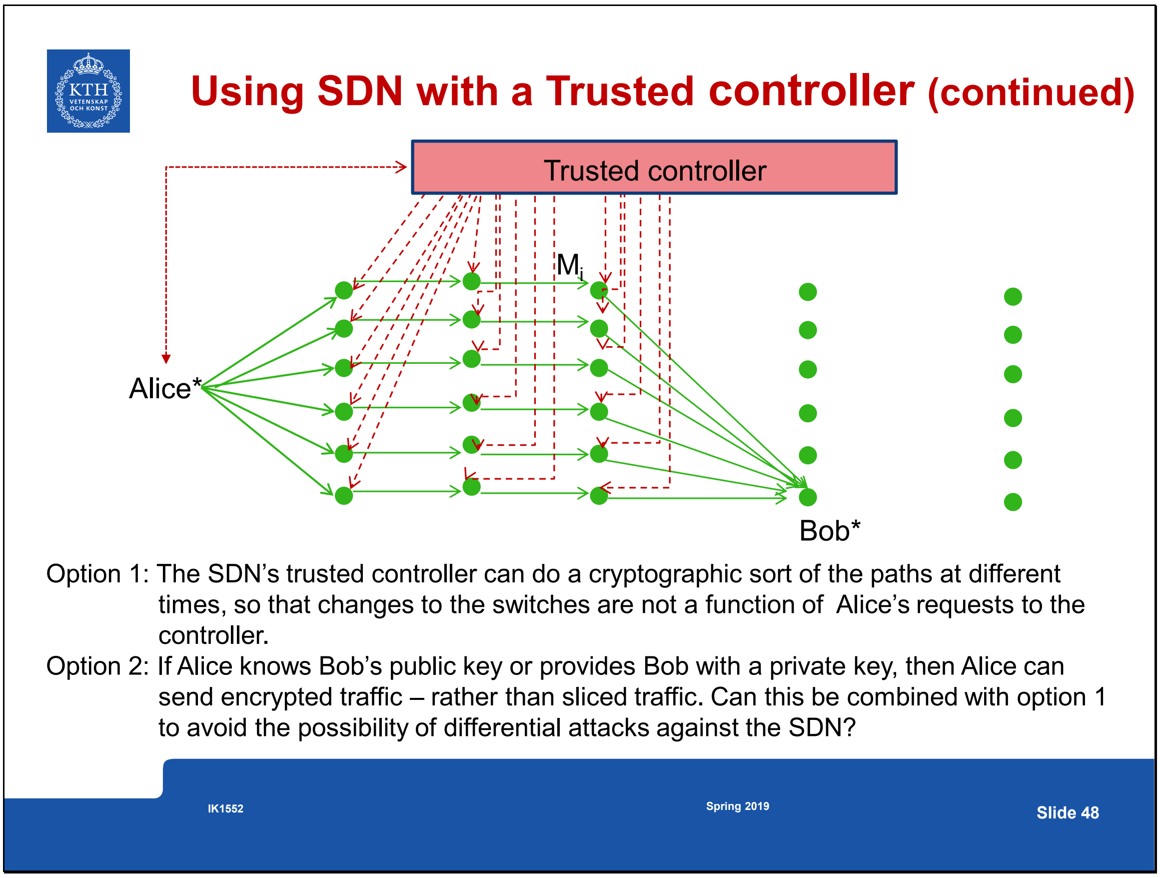
VeriSign Switzerland SA, “Integration and Treatment of VoIP and other IP-Enabled Services LI specifications”, Joint ETSI TC LI and 3GPP SA3 LI meeting, document td003, Povoa de Varzim, Portugal, 22 - 23 July 2004
http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_LI/Joint_Meetings/2004_07_Povoa/TD03%20integration.pdf

Slide 47



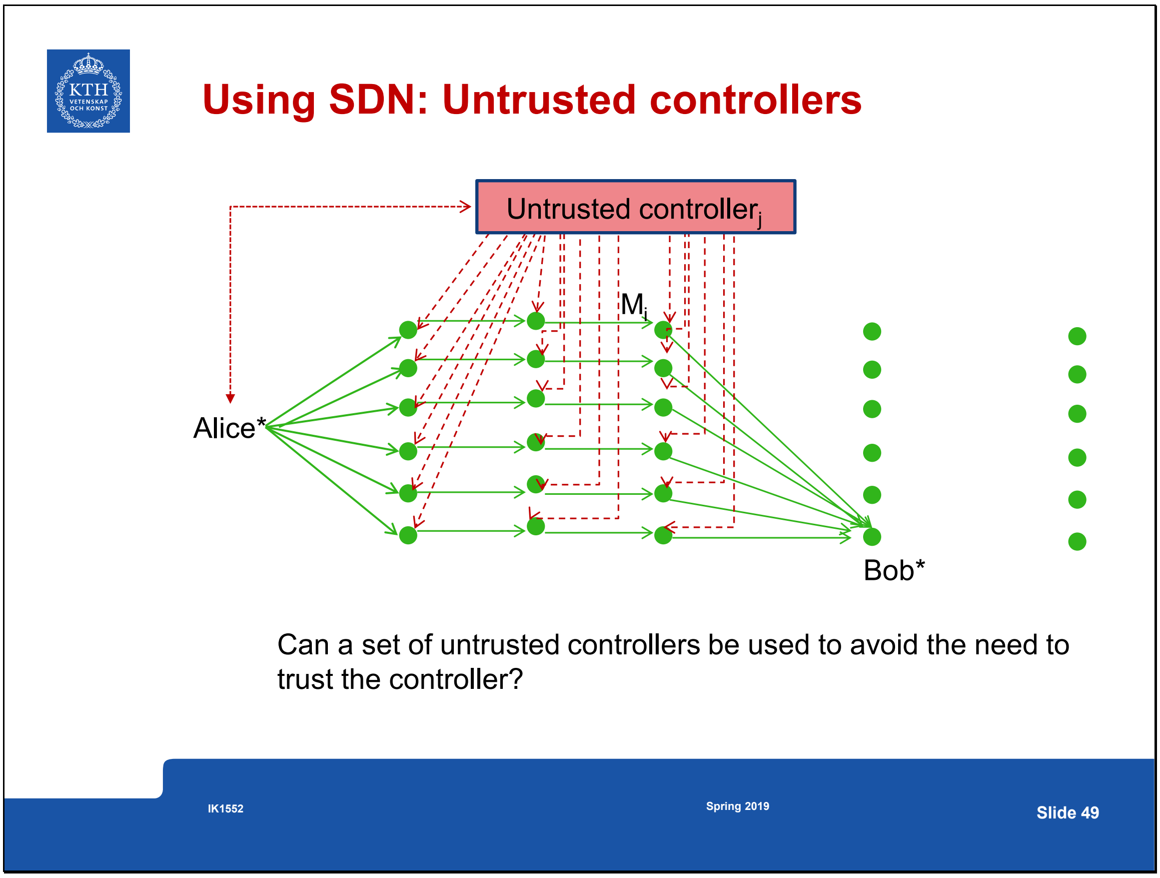
using SDNs to create anonymity networks (ala TOR or I2P) using a distributed controller. A goal would be to avoid differential timing attacks by varying the paths taken by packets from the real source to the real destination so that one does not get stationary traffic patterns that can be subject to differential delay analysis. The goal of such anonymity/pseudonymity networks to decouple source information from destination information (in a similar manner to the three hop TOR or N+/-M hop manner of I2P)

Slide 48



Using SDN with a Trusted controller (continued)
Trusted controller
M$_i$
Alice*
Bob*
Option 1: The SDN's trusted controller can do a cryptographic sort of the paths at different times, so that changes to the switches are not a function of Alice's requests to the controller.
Option 2: If Alice knows Bob's public key or provides Bob with a private key, then Alice can send encrypted traffic – rather than sliced traffic. Can this be combined with option 1 to avoid the possibility of differential attacks against the SDN?
IK1552
Spring 2019
Slide 48

Slide 49


Using SDN: Untrusted controllers
Untrusted controller$_j$
M_i
Alice*
Bob*
Can a set of untrusted controllers be used to avoid the need to trust the controller?
IK1552
Spring 2019
Slide 49

Slide 50

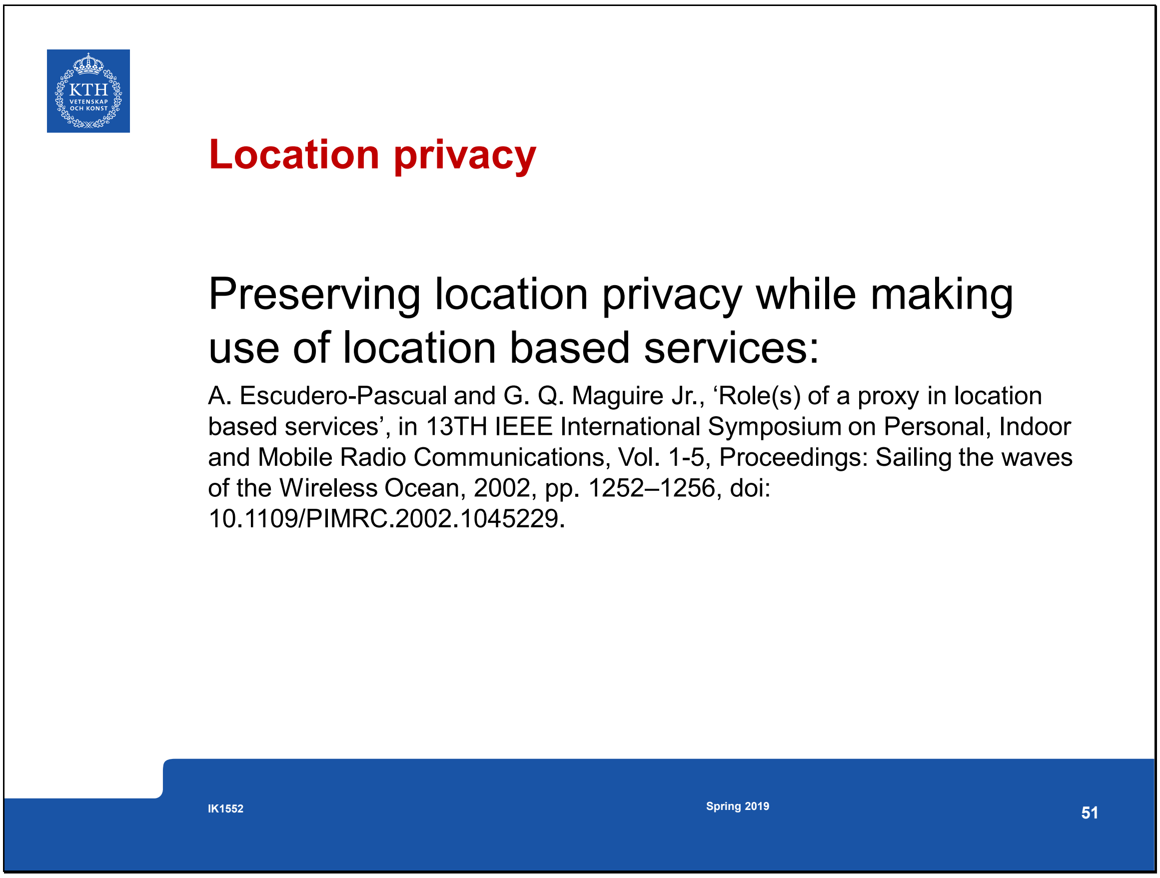
Location based services

Location based services (LBS) build upon the requirement that cellular terminals be able to be located (justified by safety purposes).

Location by the device itself or by the network

Laws regulating access to location data

Slide 51



A. Escudero-Pascual and G. Q. Maguire Jr., ‘Role(s) of a proxy in location based services’, in 13TH IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Vol. 1-5, Proceedings: Sailing the waves of the Wireless Ocean, 2002, pp. 1252–1256, doi: 10.1109/PIMRC.2002.1045229.

Slide 52

Black phones

blackphone

https://www.blackphone.ch/

FreedomPop's PrivacyPhone aka the "Snowden Phone"

http://www.freedompop.com/theprivacyphone

Boeing's Black phone –smartphone with "self-destruct"

http://www.boeing.com/boeing/defense-space/ic/black/index.page

DarkMatter's KATIM phone: https://darkmatter.ae/products/secure-communications/#products

https://www.securegroup.com/secure-phone-encrypted-communication-mobile-device/

…

Slide 53

Communications and Privacy

There are a variety of ways to:

- Protect the confidentiality of the content
- Hide the sender's location & identity

- Encryption as the **norm** ?
  - As all speech and other media will be in digital form, encryption and authentication of all communication (if the participants want to)
  - traditional "public telephony" less secure than when using: VPNs, SRTP, MIKEY, …
- Identity hiding
  - Authentication when you **mutually** want to
  - Mobile presence has to be done carefully
  - Anonymous network access What additional techniques are needed to support:
    - Traffic & Traffic pattern hiding?
    - What other paths does Alice have to communicate that do **not** pass through ISP_i (i.e., Can Alice exploit multiple ISPs to avoid problems with assumption #2).

Whom do you trust? Why?

Slide 54

Thoughts to take away

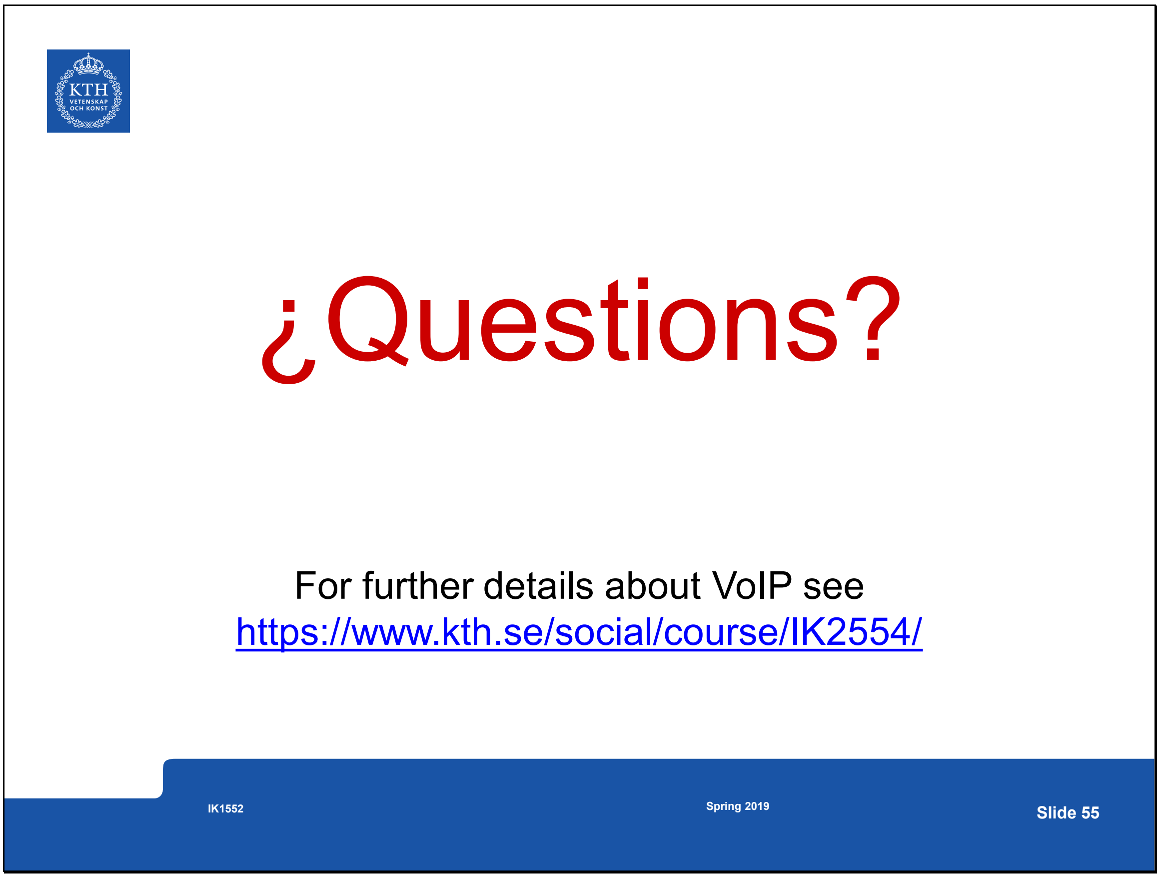
"Just because you're paranoid doesn't mean they aren't after you"

— Joseph Heller, Catch-22

"It's Not Paranoia If They Really Are Out to Get You"

— common saying, see for example: http://www.securityweek.com/its-not-paranoia-if-they-really-are-out-get-you

Slide 55


¿Questions?
For further details about VoIP see
https://www.kth.se/social/course/IK2554/
IK1552
Spring 2019
Slide 55