Privacy and Security
Purpose of the session

A conversation around where we think the Encryption issue leads to.

Share thoughts about the issues.

20 minutes introduction 20 minutes of conversation.
Background and ISOC status
And this week

US pushes Apple for access to iPhones in criminal cases

The Department of Justice would like access to an iPhone that is part of a drugs case in New York.

The US Department of Justice has said it will pursue its request for Apple to help unlock an iPhone that is part of a drugs case in New York.

A letter filed to a local court said the government “continues to require Apple’s assistance”.

And this week

SEC. 3. REQUIREMENT FOR PROVIDING DATA IN AN INTELLIGIBLE FORMAT UPON RECEIPT OF A COURT ORDER.

(a) REQUIREMENT.—

(1) IN GENERAL.—Notwithstanding any other provision of law and except as provided in paragraph (2), a covered entity that receives a court order from a government for information or data shall—

(A) provide such information or data to such government in an intelligible format; or

(B) provide such technical assistance as is necessary to obtain such information or data in an intelligible format or to achieve the purpose of the court order.
Internet Society Resources on encryption

http://www.internetsociety.org/encryption

Policy Brief on Encryption is being finalized after review period ended April 1
Directed at deployment and improving Internet scale trust infrastructure
From Encryption to System Security
ISOC’s General Principles

Encryption should be the norm for Internet Traffic

Weak Encryption is as bad as no encryption

There is a strong technical consensus in the tech community that Cryptographic backdoors are no-go territory.

Nuances

Encryption may impact operations and law enforcement activities
Encryption one tool in the security toolbox
Can a company be compelled to weaken its products security?
A few thoughts…
System Security Principles

It is my* belief that:

* This is not (yet) ISOC’s position

**Industry** is best place to assess risks, cost and benefits, and viable technical solutions hence they have a primary responsibility for their system’s security

They should be empowered to create the best possible security solutions for their products and services

Industry should, under parameters of rule of law, cooperate with law enforcement, whilst not sacrificing the principles above.

Governments should create the best circumstances for improving System Security.
System Security Principles

It is my* belief that:

Industry is best place to assess risks, cost and benefits, and viable technical solutions hence they have a primary responsibility for their system’s security

They should be empowered to create the best possible security solutions for their products and services

Industry should, under parameters of rule of law, cooperate with law enforcement, whilst not sacrificing the principles above.

Governments should create the best circumstances for improving System Security.

* This is not (yet) ISOC’s position

Not just a Law-Enforcement issue

A general Cyber Security issue

Broadly applicable

Including IOT
Some Questions and observations

Governments should create the best circumstances for improving System Security.

That means: Responsible disclosure, bug bounties, procure for security, setting high security expectations, etc, etc.

That does not mean: prevent the general public from ‘tinkering’, ‘hacking’, and security research

But how does that relate to the use of exploit kits by law enforcement?

What prevents proliferation of the tools to enable strong system security such as encryption?
Some Questions and observations

*Industry is best place to assess risks, cost and benefits, and viable technical solutions hence they have a primary responsibility for their system’s security*

For sure they are not the only actors: system security is the responsibility of many parties, including governments (public safety) and users themselves.

Collaborative Security

The responsibility of minimum standards?
Some Questions and observations

*Industry should, under parameters of rule of law, cooperate with law enforcement, whilst not sacrificing the principles above.*

What are the needs for industry to work with law enforcements and vice-versa

Additional nuance is needed. There is a difference between cooperation/assistance and becoming a tool of the government

How about the procurement and use of (existing) exploits by law enforcement?

Premise: recognize the role of Law Enforcement in public safety

Premise: recognize the role of system security in public safety
Some Questions and observations

Are the issues different for data in motion (traffic on the Internet) and data in rest (on some device)?

With encryption the norm for communication the only way to get to data is at the endpoints, which makes system security relevant to focus on.

Scoping the conversation:
Encryption, Cryptography, or System Security

Encryption is not the goal. A trusted Internet environment is.

What prevents proliferation of the tools to enable strong system security such as encryption?
Some Questions and observations

*Industry is best place to assess risks, cost and benefits, and viable technical solutions hence they have a primary responsibility for their system’s security*

Does that work in global context: what are the specific issues in cross-border cooperation?

Clearly some tension
What are your thoughts?

iipgPChPZTg94yck18astDFdSvguUT0536jBaZfuL0ZWaadw1Edoz6trK9YK13yysPcBXIRUQXRpKkI/Zs/
MhtVXKp769AZTHmaicr9VpvnXysLWupLQz9HcBTBSTFyW46v1yVevYeEBF0haP+juQ6sVU5s3N$hGmP6/TXkIdbsHSVWaIdwZvYImcBo4taNHpp9zmQd3EgyGl+60vLtpXMfIuOXLv1jw5/5znis+5cZbL5is9x7yvy6/
+iQhSuMgLEYFWGHIHIcxnOZj6AXj3b6t9xkqd37Q37WdscBR8hfoQcjwxY2nzcW7DWYtCpD0CgrLwQzR574g040te/
kz5veOrNXjQ8AUaVRh2zFJC2/+vcjcnIVnVsbl1lg764EgReNCbVx17i0+sinsjd3wiLqNwArlLW0E1i5jmFuqgQAbYxyIFCDVGf6dQPaQf6v0OJgAmzwWc6U7kXj
1R3K3DzoeOZK+fD4zZHTADwusNFPdcr3QUpk0r5X/Wl+wDnZef53Fh+eQkdjgrEvVl1fCKya9kZMSw3LaMjcl/L5c7c5R9g4q6vX6FpDguxoEjmRmVnpiW
+g0xM71luWnpBtwSgrqGElqFndSclu105gTk8TcmjQGnXcTDEJdojPlAp1Jub84cd7ndJ08vXPFQXz2CI/tNdILCRSH21ople7YWxO3k3FL
+PrtypQx5318cBWQ97g3jrj7xMyFTkghx9J53rdQxEmxNdXAs3vb+JQCAupavLu
+cmCn1SoqE4dLz56VjIrbanv1Zvityr90Rw7asNIVpPVXus6MfGj/Laviz6oJpKa7BtaNgeu/LRU1Jff/
mdzn4EcdmLOUpWznr2P133y99cTsdCvcmXsF6s1uFpqnaj/Eaara3YiwcGnvnOsk21h3WnMNwUzdvwunxwBEOuhuk5u8qsdjZhsWSDo/jkRryGsn/
32McahXQYE7KBeTD3ao8CufuV8Qjunch0sL9d9FhGqNj1xYclmQTS8QyvlkVjFPTTVylihprCmOepisNZLiuDIBXNd+zligYJ
+cDCcnlyDoGGeEKyT70q/1bg8h9j6CnxAexEagFhpR1c6nNeFud31E9neq88/tnrg4ouxNs5h6d4X5RWmEmE/
gMhQwO9900EUEo3+HdqonvQ777rZPOMpCHN92AQPVgPmXmTyF817GwFozx5Y954CC5QeH0U1+bhL7CmgMk/
+J6RM2Thvu8THdA9oAB5YfZy6wwMtkdW0uRDDkJuyAHPIvg5YQPpC5b1XEipF0oxksNP1a2jTNLCdwnu16DWYEq7Vex909qHV1yh0mCksKTZ2dp1d8gQowthyDxmAM
Pe/wC9CXvMje48HL5zj9yRorchX7B5h0dojdmik0fe6ETkagE4Q4h2wkve1sp6ELfEKMUdxA9ik2nlbLxDeN3JQzXfNsFSD0dxQgX8/
+ay8TTRWf07h8GmFoebCFg0TLxvkVr2yjumFvNrmSclFzlm3ouQahXJ+01qypHq7J9NA5hppQ0DQFWC1Qpim92Td0/bjoJIqJrlgY6YkJbXjQZtLpqj/
+suDAagQ5kbLPVaoGT3dlQUpqOpr/zJKVACnxfFWFQOQLPtPz4t03XHK2rm4kwgcVL18qzr5n3RZKUX26GPn71CmKrihiL5RilphjIXwcRsaOsvD81XUM/
QgF6h0lT1aY8b10Q01113s3p1zhu2P9Ed10y9jbo/4p+7T99vrh9k8b00q/9R910Tv60Cp885410ynFWEBdqsTQVor3GrHwzm5mqHSy5/
+D5jVj5/
G4cotMnhfUsMlilhYvLZ88LBdM3J1aMmgzK0oxsumcugQikRhVyEyui+WODyByrg51mEn/8tBipIqSohj714+PgmxAkWqG4T5SmHCcrugF748xS/0A0YIBABHh3zT/
H6R2Mu8vTh4a90a5B0v86m0ntKw0udRDKdiUyfHAPIv5YQopE00xkSNp1a2jTNLDCdnmU6DWEYqt7Vex909qHV1yhp0mCskKTZ2dp1d8gQowthyDxmAM
+4E61U4RH3Z3QqQg1jX06+doy1Nn+1/pQpgM1JuaqSet moduloQcmFcrLqgdqQl+sbsTgqZLcImYkl+n
+tdBCN5poeyVEIe0TJYرضbDavWmVnr4g5lzHJKJExLw2Akkn4k6hyQZP1KxwA6d6puf0iUjvphpEmEvKp7YFr1kH1nTvR8V7SsDS1gHrJp1ilLGExyEmhP3b/a
ecc386z8cODp4k+11gW2Q3tsLh+le08GjMIf40W7fGDJF1IR8Y7FLkx6aP5RSH5PuntuMr/nqV1q/2fxtOU+grPzMH1jB0MpwyzSc3gsZMttjhr6+0mc8g4/
EkyLg4FtHsmrU+3REHMC+YxrvsNy54a=
Olaf M. Kolkman
Chief Internet Technology Officer
Kolkman@isoc.org
twitter: @kolkman