

Cybercrime Threats and Future

Dark Musings from a Professional Paranoid

Alex Stamos, Partner

March 10th, 2009



Our Discussion Today

- Where are we today?
- Notes from the security front
 - Recent incidents
 - Interesting security research
- What needs to change?
- Predictions
- Discussion and Q&A

Who am I?

- Co-Founder and Partner at iSEC Partners, Inc.
- Application security researcher
- Fortunate(??) to experience these issues from many angles
 - Work on prominent commercial software
 - Work on open-source
 - Incident response

Where are we today?

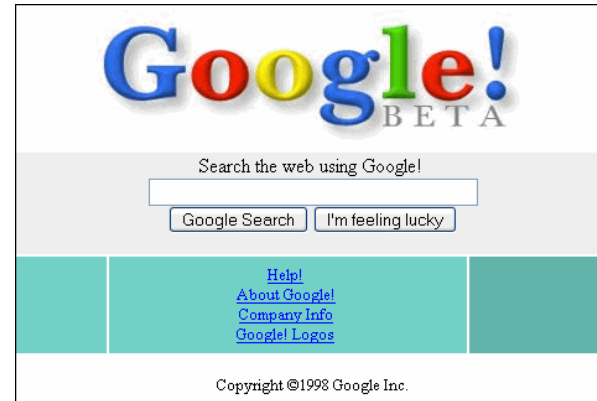
The Good

The Bad

The Ugly Truth

Need a baseline

- Let's be Base-10-centric and pick 1998



CIH Virus

DOWJONES =8,643.12

The Good

- Some software is getting better
- More parties are taking responsibility for security
- The basic knowledge for building more secure systems is out there

Some software is getting better

- Companies and products with a security process

Google™

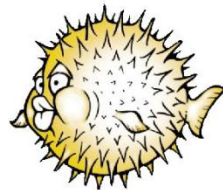
IBM®

Microsoft®



Adobe

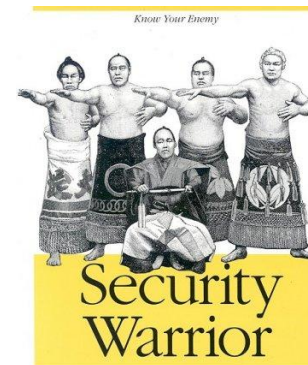
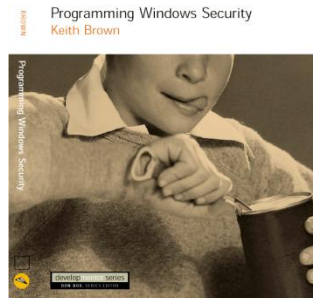
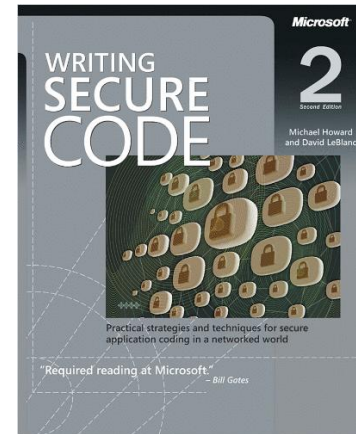
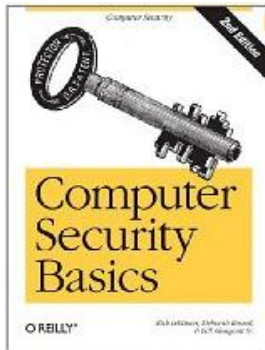
ORACLE®



OpenBSD

Security Knowledge

- Engineers have many more resources at their fingertips



The Bad

- The software that's getting better only reflects a small fraction of the ecosystem
- Computer crime has become professionalized
- Law enforcement is doing better, but not good enough

Professionalization

Remember these?



THIS SITE IS HACKED BY 'THE HACKMASTERS'

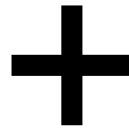
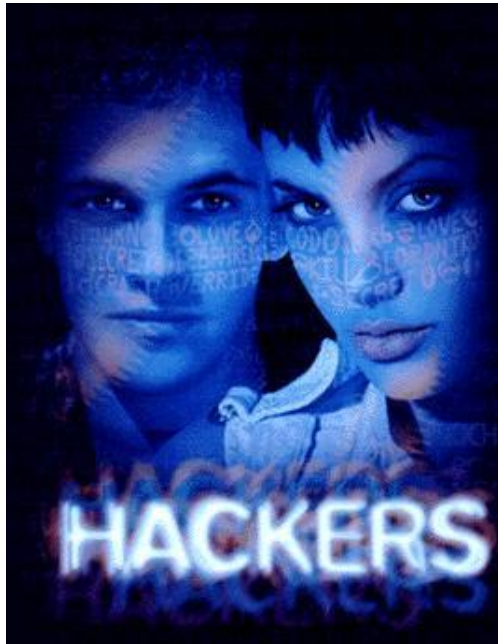
Greetzzzzzz to: LittleAnGel, the MaNiac, Pudding and to MySelf

BTW: Stealth is a LOSER!

<http://www.flashback.se/hack/1998/11/25/1/>

Professionalization

Now we've moved on to...



Professionalization

- Online markets
 - Iceman takes control of market, gets busted
 - Great [story](#) on DarkMarket FBI sting
- Semi-automated identity theft
- Cross-border collaboration
- Immunity from local prosecution

International Issue is Key

- It's pretty easy to hide your identity while hacking on the Internet
- If you live in .cn, .ru, or .ro it might not be necessary
- USSS and FBI have improved their contacts in these countries, but...
- For the most part, prosecution or evidence gathering in many places is impossible, giving criminals free reign

Mixture has changed



<http://www.ic3.gov/media/annualreports.aspx>

The Ugly Truth

- The Internet cannot be safely used by most users
- Technological improvements have diminishing returns
- The security industry is failing you (sorry)

News from the security front

Incidents

Research

Recent Incidents

- Many important incidents are still not reported
- Those you have heard of...



94M Credit Cards



80K LEO Identities



100M+ Credit Cards

Heartland

- Processes CCs for 200K businesses, 100M transactions per month
- Announced on Inauguration Day. That's PR strategy!
- Liability outcomes will be interesting, Heartland is probably toast
- What can we learn?

Heartland and PCI

- Heartland has raised questions about the most important private regulatory framework



- Had a valid PCI DSS certification from Trustwave
 - Now being sued by victims, ala Arthur Andersen
- Perhaps the "Audit Model" doesn't really work for InfoSec?

Future of Payments

- Maybe the credit card model is dead, we just don't know it
- What does a credit card hold?
 - CCN
 - Name
 - Exp Date
 - Billing Zip
 - CVV₂
- Where's the secret? Where's the crypto?

Recent Research

- Security researchers have been tearing down basic Internet infrastructure
- First, this man ruined your DNS cache

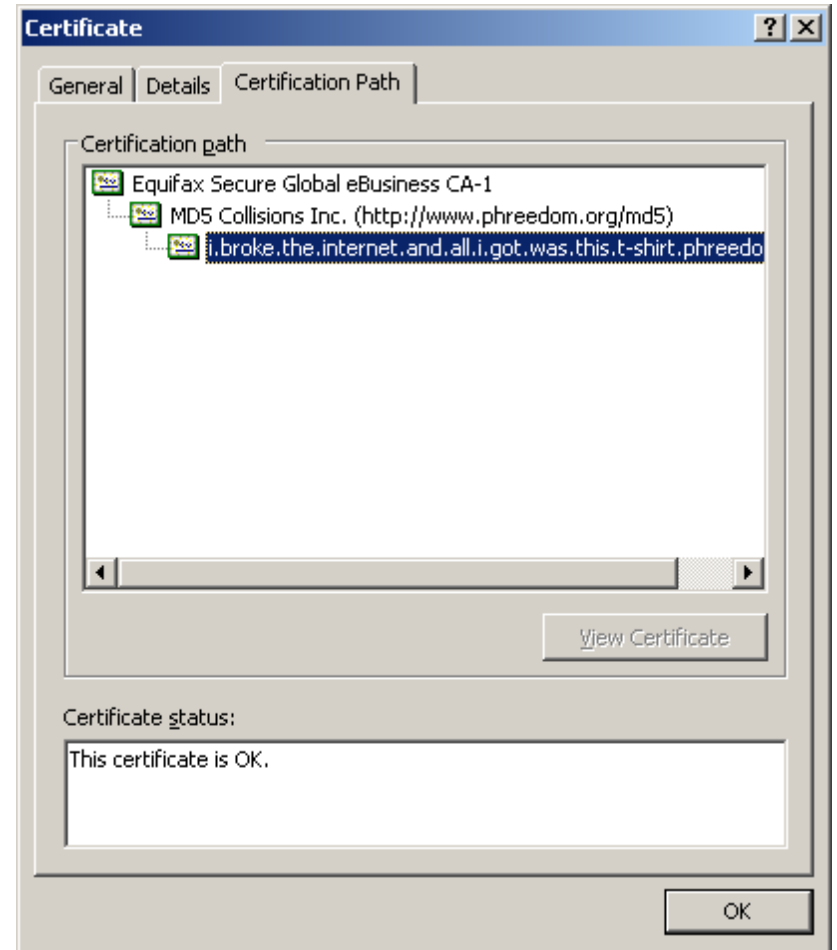


Recent Research

Then, these guys:



Made this:



Other important research

- Heap manipulation with JavaScript (Sortirov)
- Flash hybrid exploit code (Dowd)
- Cold (really cold) boot attacks (Halderman et. al)
- Clickjacking (Grossman and Hansen)

Recent Research

- What trends do we see?
- Most interesting research is either:
 - Making the unexploitable exploitable
 - Breaking down basic building blocks from the 70s and 80s
- Lessons:
 1. Never say “that can’t be exploited”
 2. If it’s older than you, don’t trust it

What needs to change?

Security Industry

Software Engineering

Safety and Choices

Patching

Security as an industry is failing

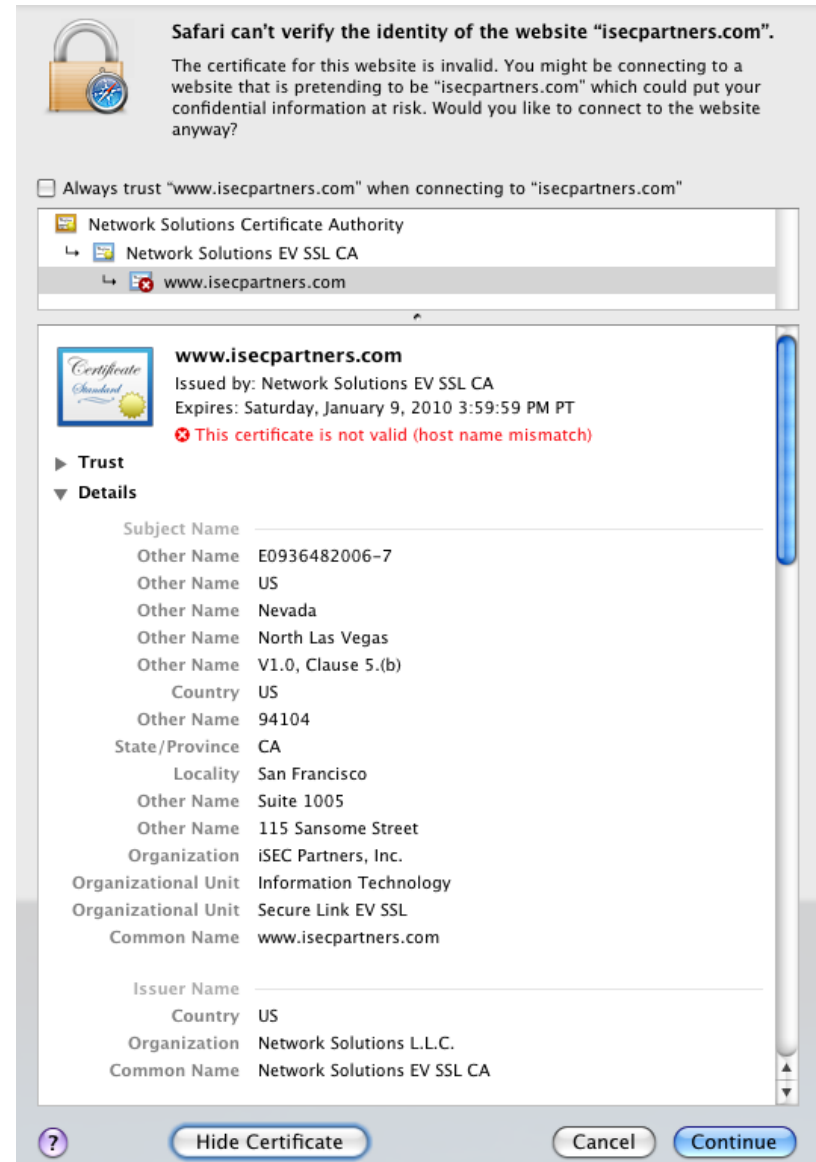
- 20 some years of security “professionals” and things are even worse
- Why?
 - Still more rewards for breaking things
 - Every solution gets turned into an over-priced, marketing driven \$500K product
 - Industry is tiny rudder on huge ship of software engineering

Software Engineering

- Still not really engineering
- Important time is first 2-3 years of professional experience
- Knowledge is available, just not being used
- Why are people using unsafe languages and constructs?

Safety versus security

- Time to stop asking users to make decisions they are not qualified to make:



Safari can't verify the identity of the website "isecpartners.com".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "isecpartners.com" which could put your confidential information at risk. Would you like to connect to the website anyway?

Always trust "www.isecpartners.com" when connecting to "isecpartners.com"

Network Solutions Certificate Authority
Network Solutions EV SSL CA
www.isecpartners.com

www.isecpartners.com
Issued by: Network Solutions EV SSL CA
Expires: Saturday, January 9, 2010 3:59:59 PM PT
✘ This certificate is not valid (host name mismatch)

► Trust
▼ Details

Subject Name _____
Other Name E0936482006-7
Other Name US
Other Name Nevada
Other Name North Las Vegas
Other Name V1.0, Clause 5.(b)
Country US
Other Name 94104
State/Province CA
Locality San Francisco
Other Name Suite 1005
Other Name 115 Sansome Street
Organization iSEC Partners, Inc.
Organizational Unit Information Technology
Organizational Unit Secure Link EV SSL
Common Name www.isecpartners.com

Issuer Name _____
Country US
Organization Network Solutions L.L.C.
Common Name Network Solutions EV SSL CA

? Hide Certificate Cancel Continue

Let me fix that



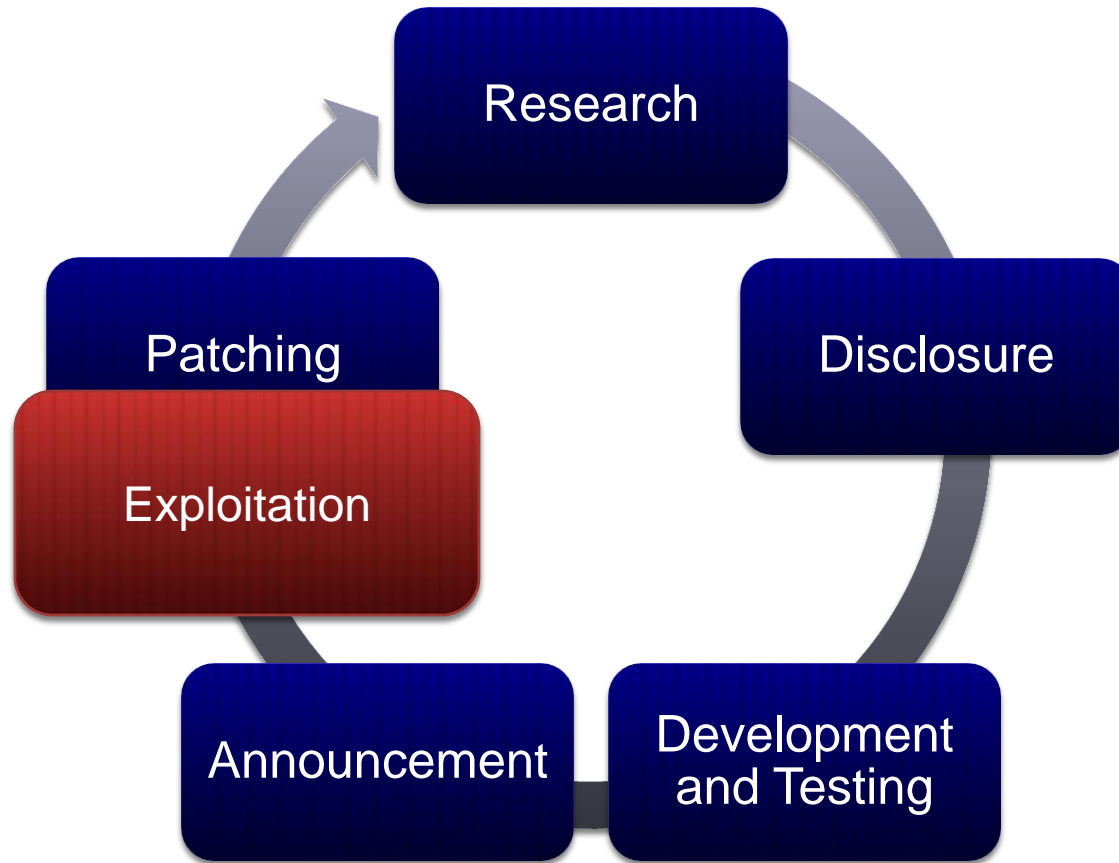
Safari can't verify the identity of the website "isecpartners.com".

Thanks, but no. You're done.

Cancel

Patching

- The old vulnerability disclosure cycle is failing



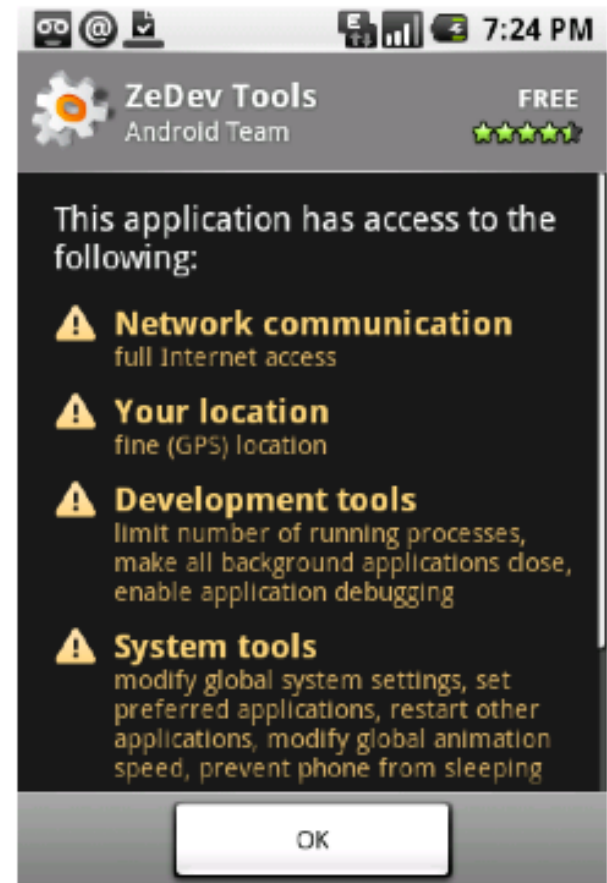
Patching

- Patching has been the most important end-user security step
- Users fail to do it all the time. Again, time to stop asking questions
- Look at your screen, do you see these?



Desktop user model

- The standard OS user model is also failing
 - Based upon Unix multi-user model
- Most desktops only have one user anyway, making most OS protections useless
- Leadership from the mobile space:



The Future

Predictions

- Now for the key part of an ETech talk, totally unfounded predictions...
- So, In the Year 2000....



Basic Infrastructure Failure

What's next?

- BGP is terrifying
- DNS is still scary
- Mixed HTTP/HTTPS web sites are toast
- SHA-1 is in rapid decline
- MD5 Collision attacks will be useful elsewhere

Social Network Madness

- Social network sites are already great for stalkers
 - Location awareness fad will end with a horrible tragedy
- Social networks are ruining “two factor authentication”.
Breaking into my bank account?

Where did you go on your honeymoon?

- Hmm, go to Facebook, pull the photos, and guess:



Mobile Devices

- Lots of challenges here, see C. Clark at RSA
 - Still, it's a chance to reboot how security is done
- Screen Real Estate makes security UI difficult:



(a) Real Chrome



(b) Fake Chrome

Web Security

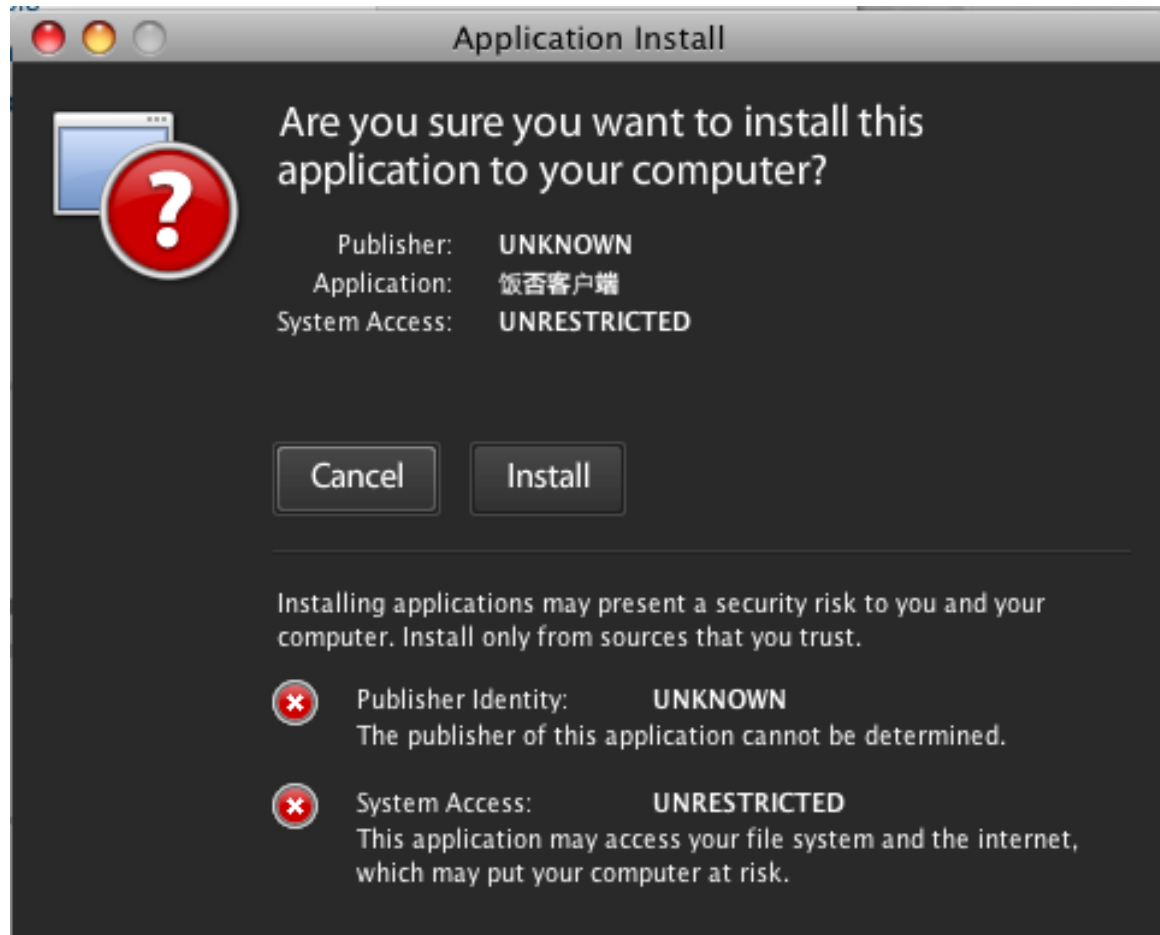
- There is no browser security model.
- Browser continues to be the most important attack surface on the computer
- W3C is making things worse, by

Rich Internet Applications

- We did a whole talk on this last year...
- Fun with:
 - Client side SQL injection!
 - Theft of offline data!
 - Web XSS turning into control of the desktop!
 - Cross platform malware!
- Yeah! Totally necessary!

Rich Internet Applications

- Get ready for this prompt:



Real Human Impact

- Next 20 years will show the impact from lack of law enforcement in some developing countries
- Companies are already blacklisting certain ASes
 - Double-digit percentage of users in some countries are fraudsters
- Will this generation of young Internet users be willing to collaborate with entrepreneurs from high-fraud countries?

Conclusion

- It's a good time to be paranoid. They ARE out to get you!
- Security industry needs a good look at itself
- Prepare for a post-privacy post-security society

Thank you for coming

Q & A

alex@isecpartners.com