A little security discussion

Jon Jensen
End Point Corporation
19 October 2012

Please take notes for yourself!

Let’s start from the inside.

Your physical office

- Locked windows & doors
- Paper out on desk
- Paper filed away
- Paper in trash or recycling
- Backup hard disks
- USB thumb drives
- WiFi sniffing
- Classical eavesdropping
- Screen locking

Your physical offices, plural

- Home
- Separate office
- Friend’s place
- Café, other businesses, school, church
- Travel: hotel, airport
- Laptop and desktop?

Smartphone: all the same concerns and more

- Easiest to lose or have stolen
- Email always logged in?
- Web browser runs forever, cookies still usable
- Screen locking
- SD card removal
- USB hacking
- Run up charges for SMS, apps, int’l calls, etc.
- Google Authenticator or other secrets apps

Your personal soft valuables

- PGP and ssh private keys
- Google account: Calendar, Docs, Contacts, Gmail, AdWords, Voice, App Engine, Compute Engine, Play Store, G+, Picasa …
- End Point accounts: email, firewalls, wiki, RT, timesheet, IRC, etc.
- Server accounts on End Point & client machines
- Sensitive web logins: GitHub, Dropbox, cloud hosting providers, Interchange admin, Spree admin
- Services tied to credit cards: ISP, Skype, cell phone, bank accounts, PayPal, Amazon.com, Orbitz, …
- Client's & your own credit card or banking info
- Domain names

Your clients’ soft valuables

- Domain names
- Source code: on GitHub, their servers, our servers, your workstation, backups
- Business secrets, plans, sales data
- Customers’ personal or buying details
- Medical or financial data
- Good reputation and customers’ trust

End Point's soft valuables

- The intersection of yours and all our clients'
- Our good reputation and clients' trust
- Our own business data
- Our own company accounts
- Our own servers
- All our super-seekrit open source software ☺

Weak link in the chain

- Attackers only have to win against the easiest targets
- Automated attacks are cheap
- Never know what they might want, or when
- Constant vigilance

Possible consequences of a breach

- Hardware loss = money, downtime, data loss
- Fraudulent credit card charges
- Unwilling botnet zombie
- Bad public relations
- Lawsuits for negligence
- Loss of business, clients
- Increased insurance costs

What are you doing to protect yourself?

What more can you do?

What/who are the threats?

Think like an attacker

Basic rules

- Don’t put important passwords or credit card info in email, IRC, SMS, RT, wiki, timesheet
- Shred, burn, or tear paper secrets to small pieces
- Politely help clients to be more secure, but don’t insist brusquely on our same standards; losing battle
- Leave SSL keys in place where they were created; otherwise should only be in backups
- Generate PGP keypairs on workstation, not servers, e.g. for encrypting ecommerce data

Must haves

- Run a desktop screen locking app, both to use on demand and by timer
- Use different passwords for everything important
- Never store PGP or ssh secret keys on our servers

Strongly recommended

- Google Authenticator 2-factor auth
- Full-disk encryption on your main computer
- Use phone lock screen, or don’t keep anything important on it
- Full-disk encryption for backups, or cloud backups

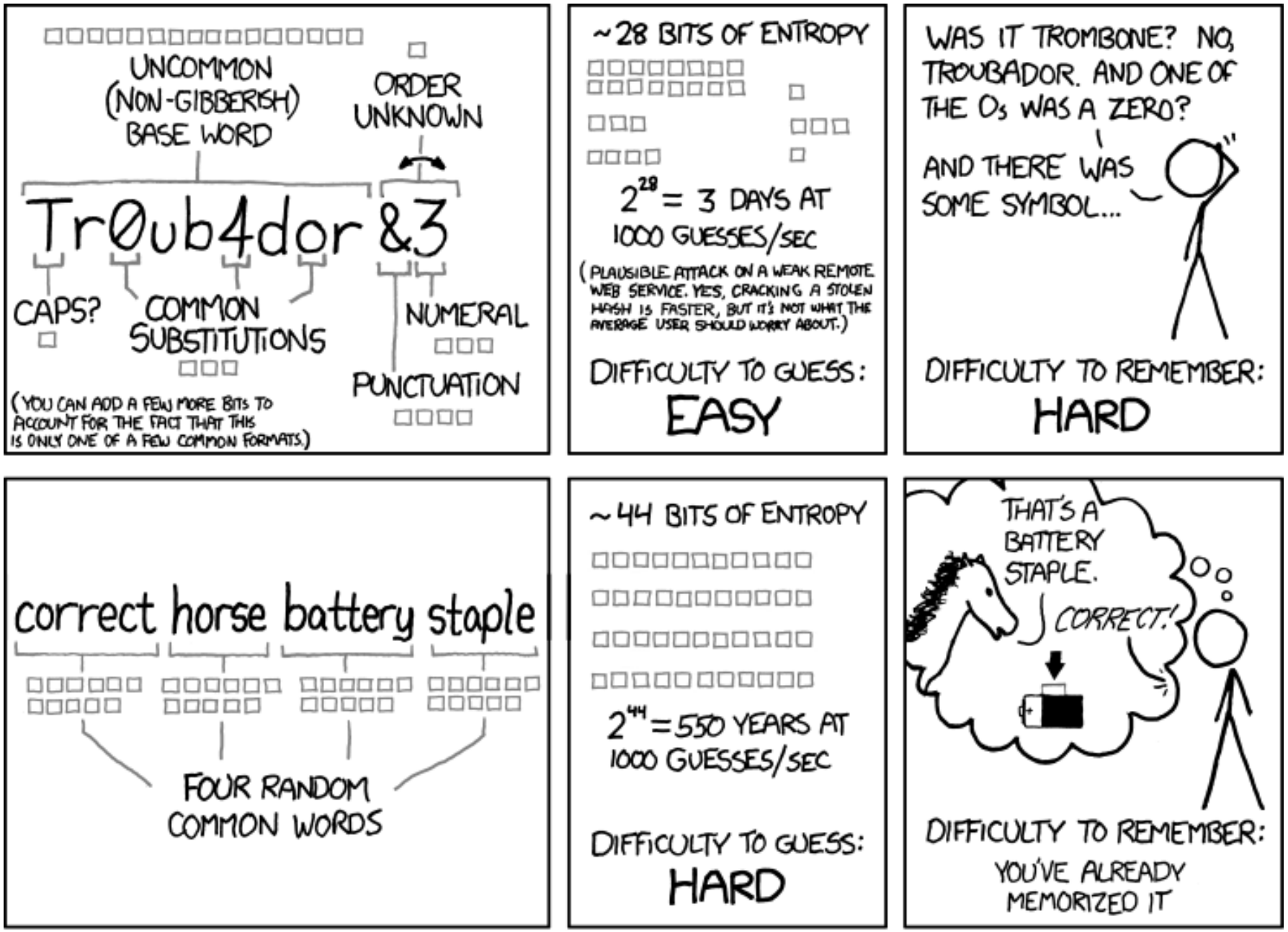
Also good

- Normally use a more secure browser or profile without Java, Flash, PDF
- Avoid using browser password storage
- Use apg or similar to generate passwords
- Use a different computer for proprietary or downloaded stuff like games

Passwords

Use APG for passwords you don’t have to remember.

But:



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Readings

- Bruce Schneier's Crypto-Gram and books
- Security testing (Wikipedia)
- Security Concepts online book
- Protecting a laptop from simple and sophisticated attacks (Mike Cardwell)
- Talks from DEF CON, HOPE, CCC, etc.

The end of the beginning