Psykologi och social engineering

Daniel Bosk[1]

Avdelningen för informations- och kommunikationssytem (IKS),
Mittuniversitetet, Sundsvall.

psycho.tex 1674 2014-03-19 14:39:35Z danbos

Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)

Kaufmann, Perlman and Speciner

Översikt

1. Psykologi
   - Social engineering
   - Grundläggande psykologi
   - Socialpsykologi
2. Autentisering
   - Lösenord
   - Bättre lösningar?
3. Advanced Persistent Threat (APT)
   - Vad är APT?

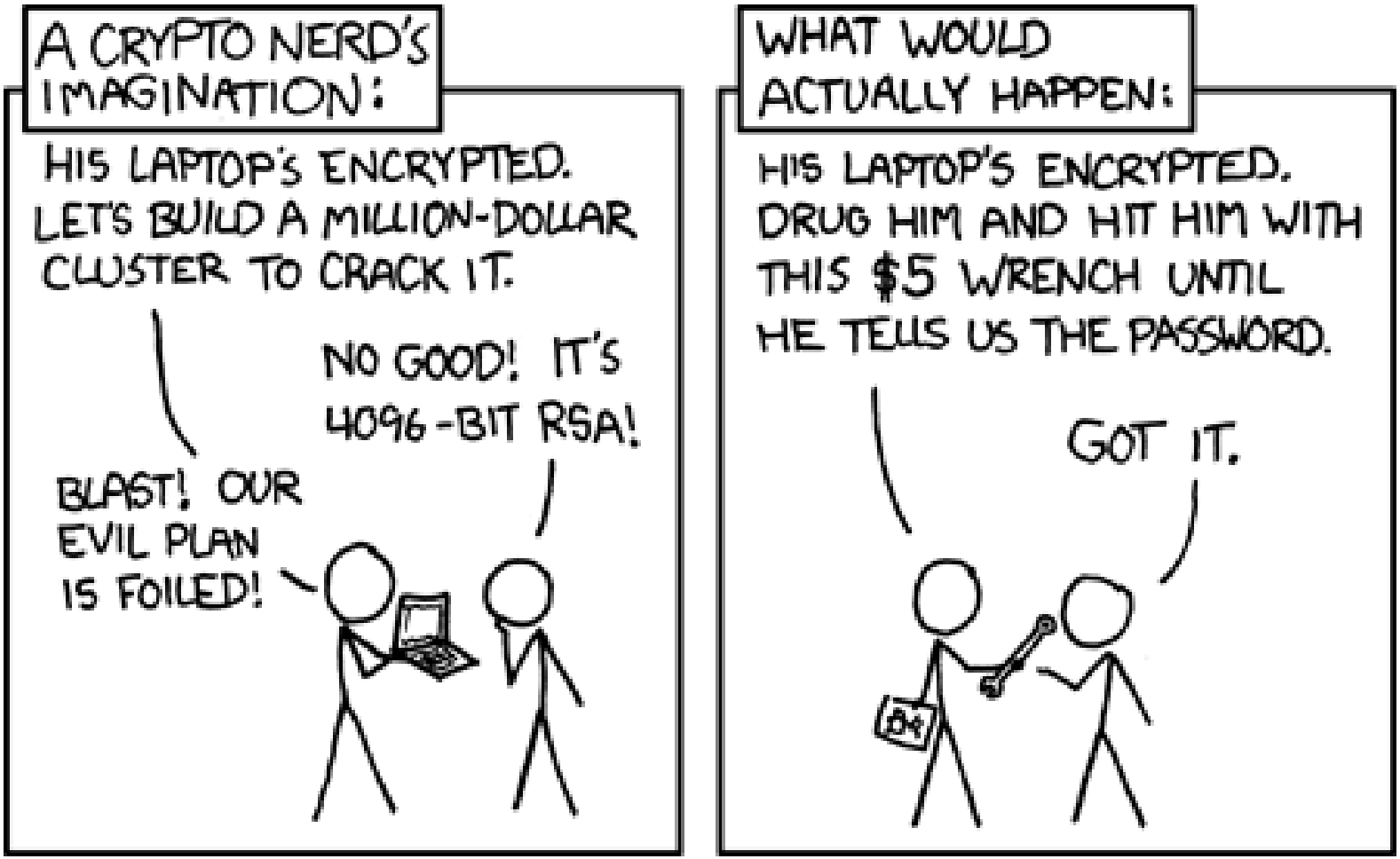
Litteratur

One important aspect of security, which traditionally is forgotten, is the users' weaknesses. The psychology of the human mind is therefore an important subject to discuss in the context of security. Anderson gives a short summary of the psychology of users, their strengths and weaknesses, in chapter 2 "Usability and Psychology" in [And08].

Översikt

Översikt

Social engineering



Figur : "Only amateurs attack machines; professionals target people." (Bruce Schnier). Bild: [xkcc].

Social engineering
Vårt naturligt utvecklade skydd

- Vårt naturliga skydd som utvecklats under miljontals år är baserat på ”här och nu”.
- Hotet har bytt kontext under de senaste decennierna.
- Evolutionen är betydligt långsammare . . .

Social engineering
Pretexting

- Att ringa någon som har tillgång till informationen och låtsas vara behörig att få veta.
- Exempelvis att låtsas vara behandlande läkare av en patient i en akut situation för att få ut information ur journalen.
- Från verkligheten [And08]: Ett falskt pressmeddelande publicerades som sade att VD avgått och att vinsten skulle räknas om.
  - Aktien föll med över 60 % innan det uppdagades.
- Generellt går denna typ attack under *social engineering*.

Social engineering

- Undersökning genomfördes i UK 1996 [And08].
- Utbildade personalen vid vårdinrättning om pretextingattacker.
- Upptäckte 30 falska samtal i veckan.

Social engineering

- Vid granskning av IRS 2007 ringdes 102 personer spridda över hela organisationen upp.
- De ombads uppge sitt användarnamn och ändra sitt lösenord till ett givet värde.
- 62 av dem följde instruktionen.

Social engineering

- Användare säljer sina lösenord för en chokladkaka [TT10].
- Personer tar främmande USB-minnen och använder dem med sina datorer.
  - Närmare bestämt 46 % av ekonomicheferna vid 500 börsnoterade företag [**?**].
  - 66 % innehåller sabotageprogram [Duc11].

Social engineering

- Militära organisationer har alltid haft varandras personal som måltavla för denna typer av attacker.
- De har fördelen att kunna utbilda sin personal.
- Vanliga organisationer kan också utbilda sin personal.
- Det blir desto svårare att utbilda kunder eller andra personer som berör verksamheten men inte är en del av organisationen.

Social engineering
Phishing

- Det är inte längre organisationen som angrips utan kunder och personer runt omkring.
- Angripare återanvänder riktiga e-brev med utbytta URL:er.
- Vill ha ut användarnamn, lösenord, personuppgifter, ...

Råd

- Klicka aldrig på URL:er som skickats till dig.
- Skicka aldrig klickbara URL:er till någon.

Social engineering

Mat Honan of Wired Magazine

Vad?

- Angripare tog över och tog bort Googlekonto.
- Tog över Twitterkonto och postade kränkande kommentarer.
- Tog över AppleID-konto och tog bort alla data från alla Apple-enheter.

Hur?

- Brister hos Amazon.
- Brister hos AppleCare.
- Olycklig koppling av e-postadresser för Me.com och Gmail.
- Detta gav dem även Twitter.

Översikt

Grundläggande psykologi

- Mentala modeller som låter oss identifiera människor, ljud, ”koncept” bättre än datorer.
- Dock gör oss även sårbara när fel modell aktiveras.

Grundläggande psykologi

Capture errors

- Ett inövat beteende används istället för korrekt.
- Svänger ut på motorvägen mot Sundsvall istället för Härnösand.
- Åker hem istället för till affären efter jobbet.
- Klickar ”automatiskt” på OK-knappen utan att tänka efter.

Post-completion error

- När målet är nått är uppgiften genomförd, eller . . .
- Uttagsautomater som ger pengarna före kortet gör att fler glömmer kortet i automaten.

Grundläggande psykologi

- Handlingar som följer någon form av regel.
- Vid hög kognitiv belastning kan fel regel följas, exempelvis starkaste regeln istället för lämpligaste.

Exempel

- Det är säkert då det står ”https” i URL:en, eller ikonen med hänglåset.
- Att hitta bankens namn är en starkare regel än att tänka på dess position;
  `https://www.swedbank.se.fraudulentbanks.com`.

Grundläggande psykologi

Figur : En kort seriestrip om hur vi är okritiska mot text som, till synes, har referenser. Bild: [xkca].

Grundläggande psykologi

- Heuristiker människor använder för beslut ligger på gränsen mellan rationellt tänkande och direkta sinnesintryck.
- Risker: I många fall tycker vi mindre om att förlora $100\ \mathrm{kr}$ vi redan har än att vinna $100\ \mathrm{kr}$ vi inte har.
  - Marknadsföring: ”spara $100\ \mathrm{kr}$”.
- Vi är dåliga på att uppskatta sannolikheter:
  - Baserar härledningar på enkla analogier.
  - Tillgänglighetsheuristiken: lättillgängliga data har större vikt vid resonemang.
  - Och vi jämför med nyliga händelser.
  - Förankringseffekten: vi gör en initial uppskattning och förbättrar vid behov.

Grundläggande psykologi

- Vi är mer benägna att vara skeptiska mot något vi hört än något vi sett.
- Överskattar risken för terroristattacker jämfört med bilolyckor.
- Beror dels på synligheten i media.
- Gilbert: ”If only gay sex caused global warming”.
- Global uppvärmning bryter inte mot någons (religiösa?) värderingar, är långtgående hot.
- Vi är anpassade för snabba förändringar i omvärlden och tydliga akuta hot.
- Vi är också mindre rädda när vi (tror) att vi har kontroll, exempelvis att köra bilen jämfört med att sitta som passagerare.
- Vi är också riskaversiva: ”kvitt eller dubbelt” går inte hem.

Grundläggande psykologi

- Kan dela upp psyket i kognitivt och affektivt system.
- Utvecklingsbiologin har sett att olika processer används för sociala och fysikaliska fenomen.
- Barn försöker att förklara händelser med sin förståelse för fysik, när den inte räcker försöker de förklara med avsiktliga handlingar (det affektiva tar vid).
- Detta leder till att de tar hjälp av vuxna.

Grundläggande psykologi
Bieffekter

- Människor försöker att förklara händelser med intention snarare än situation.
- Vidare leder detta till att om vi får den affektiva sidan att ta över är personen mindre uppmärksam och sämre att uppskatta sannolikheter.

Grundläggande psykologi

- Två studier visar att tilliten till resultaten från Google är stor.
- Studenter valde länkar högre upp i träfflistan trots att sammanfattningarna var mindre relevanta än träffar längre ned [PHJ+].
- I en nyligare genomförd studie [ER13] visas att sökresultat kan förändra personers röstningspreferenser utan att uppmärksammas.
- Detta gör sökmotoroptimering till ett farligt område.

Översikt

Socialpsykologi

- Det sociala samspelet har stor inverkan på individen.
- 1951 visades att en individ kunde bortse från uppenbara bevis bara för att följa gruppen.
- Vidare har visats att individer kan göra helt moralvidriga saker under order från en auktoritet, Officer Scott 1995–2005:
  - Ringde upp restaurangchefer och låtsades vara polis.
  - Tvingade fram strippsökningar av oskyldiga unga anställda.
- Detta kan ske även utan order från en auktoritet, Stanford Prisoner Experiment 1971:
  - 12 vakter, 12 fångar.
  - Vakterna blev snabbt sadistiska auktoriteter.

Socialpsykologi

Sociala medier?

Socialpsykologi
Kognitiv dissonansteori

- Människor tycker inte om motstridigheter.
- Söker information för att bekräfta tidigare kunskap eller mentala modeller.
- Information som motstrider bortses ifrån, vill inte tro att man tidigare haft fel eller bryta från alla andra.

Översikt

Mittuniversitetet
MID SWEDEN UNIVERSITY

Översikt

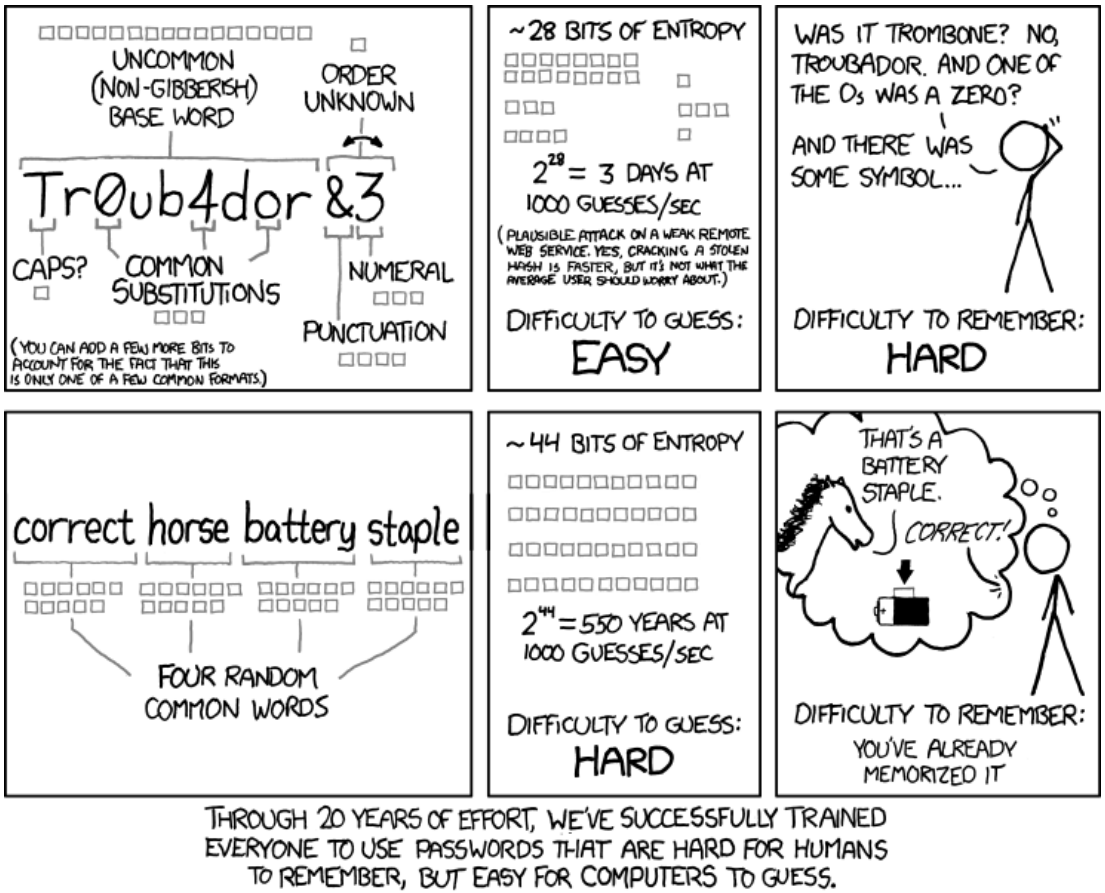
Lösenord
Användbarhet?

- Svårt att komma ihåg detaljer som används sällan.
- Svårt att komma ihåg detaljer som ändras ofta.
- Svårt att komma ihåg och särskilja många liknande detaljer.
- Svårt att minnas ord utan betydelse.
- Kan ej glömma på begäran.
- Att minnas är svårare än att känna igen.

Lösenord

- Enklare att komma ihåg saker som används ofta.
- Enklare att minnas saker i kontext.
- Men . . .

Lösenord



Figur : "To anyone who understands information theory and security and is in an infuriating argument with someone who does not (possibly involving mixed case), I sincerely apologize." [xkcb] Bild: [xkcb].

Lösenord
Alternativ

Något du har, något du vet, eller något du är.

Eller enligt Simson Garfinkel:

Something you had once, something you've forgotten, or something you once were.

Lösenord
Alternativ?

Vet	Lösenord.
Har	Koddosa, som oftast skyddas av ett lösenord.
Är	Fingeravtryck, som oftast kombineras med ett lösenord.

Lösenord

Komplexiteten hos lösenord

- PIN-koden för betalkortet, har endast tre försök sedan slutar kortet att fungera.
- Lösenordet för webbmailen, vore väldigt jobbigt om den blev låst. Hur låsa upp?
- Krypterat data, har ej kontroll över antal försök.

Lösenord

Andra typer av lösenord

- Personnummer (även användarnamn).
- Kortnummer, medlemsnummer.
- Husdjurets namn.
- ”Mother’s maiden name”.

Lösenord

Säkerhetsfrågor

Figur : En seriestrip som antyder det bisarra med säkerhetsfrågor. Namnge dina husdjur med omsorg, du kommer att använda deras namn som säkerhetsfråga resten av livet.

Lösenord
Problem att lösa

1. Kommer användaren att mata in rätt lösenord tillräckligt ofta?
2. Kan användaren minnas lösenordet, eller kommer denne att skriva ner det på en lapp? Väljer användaren ett lösenord som är lätt att gissa?

Lösenord

Att mata in lösenord

- Muntligen ange ett nummer: hotel-, biljettbokningar, hämta ut paket från Posten.
- Mata in långa sifferkombinationer: mjukvarulicenser, refillkort, OCR-nummer för räkningar.
- Att skriva dem i grupper om tre till fyra underlättar avsevärt.
- Längre lösenord, större sannolikhet att skriva fel.

Lösenord

Att komma ihåg lösenord

- Välj ett lösenord du inte kan minnas och skriv inte ner det.
- xkcd:s ”correct horse battery staple”, enkelt att komma ihåg men svårt att skriva.
- xkcd:s ”Tr0ub4dor&3”, går att lära sig skriva utan fel men svårt att komma ihåg.

Lösenord

Lösenord från verkligheten

Från [Obe10]:

- 123456
- password
- 12345678
- qwerty
- abc123

Från [Clu12]:

- 123456
- password
- welcome
- ninja
- abc123

Lösenord

Lösenordspolicy

Vi får se i [KSK+11] att ”minst 16 tecken” är den bästa lösenordspolicyn.

Lösenord

Attackera ett konto eller alla

Ett givet konto

- Svårt med lösenordsknäckning, måste testa $|P|/2$ där P är mängden av alla lösenord.
- Med phishing kallas detta *spear phishing*.

Alla konton på ett system

- Avsevärt mycket enkare, närmare $|P|/|U|$ där U är mängden av användare.
- Kan använda phishing, räcker med att en användare faller för det.

Alla konton på alla system

- Knäck lösenord för ett enkelt system.
- Phishing för ett system med dåliga policyer.
- Sannolikt återanvänds lösenord i andra system.

Lösenord
Användarträning

- Träna användare att använda säkra lösenord.
- Ge dem säkra lösenord.
- Värdera lösenordet lika starkt som det som skyddas.
- Ge negativ återkoppling på dåliga lösenord.
- Låt vakter gå runt på kvällen och städa undan eventuella lösenord nedskrivna på lappar.
- Men begär inte något de inte klarar av, då kommer policyn aldrig följas.

Lösenord

Användarträning – social engineering

- Marknadsföringsavdelningen vill skicka länkar.
- Var konsistent, ge inte användaren delade budskap.
- Låt dem inte göra det om ni försöker att träna användarna att använda bokmärken eller skriva URL:en.
- Outsourceade kundundersökningar: från er(?) men med konstiga URL:er. ”There’s something phishy going on.”

Lösenord
Trusted Path

- Vi måste veta om vi kan lita på kommunikationskanalen.
- Är det ett riktigt tangentbord, eller är det utbytt mot ett som sparar alla tangenttryckningar?
- Är det en genuin kortterminal?

Översikt

Bättre lösningar?

- Lösenord är har i sig dålig användbarhet.
- Finns olika metoder för att förbättra användbarheten.
  - Single sign-on, exempelvis via Google eller Facebook.
  - Spara alla lösenord krypterat och fyll automatiskt i dem på webben.
  - Komplettera med koddosa.
- Då har vi reducerat N lösenord till endast ett lösenord att komma ihåg.
- BankID verkar vara en robust lösning, kan vi inte använda den?

Bättre lösningar?
BankID

- Innebär att vi måste ha någonting: certifikatet.
- Vi måste veta någonting: lösenordet för certifikatet.

Bättre lösningar?
BankID hos Swedbank

Inloggning

I identify myself at:
Swedbank och Sparbankerna

Godkänna (signera) överföring

I sign at:
Swedbank och Sparbankerna

Text to be signed:
Jag godkänner överföring med totalsumman 60,00 kr. Uppdraget lämnar jag till banken 2013-04-14 kl 21:25:43.

Bättre lösningar?
BankID hos Skatteverket

Inloggning

I identify myself at:
Skatteverket

Signering av deklaration

I sign at:
Skatteverket

Text to be signed:
Härmed undertecknar jag uppgifterna jag tidigare lämnat in.

Bättre lösningar?
BankID

- Har separata mekanismer för identifiering och signering.
- Kan alltså inte lura användaren att signera en överföring vid inloggning.
- Har ett användbart och pålitligt användargränssnitt.
- Jämför med användargränssnittet till chippet på betalkortet (precis, det finns inget).

Bättre lösningar?

Utforma autentisering för att användaren inte enkelt ska kunna bli lurad!

Översikt

Översikt

Vad är APT?

- Ett påkostat angrepp.
- Pågår under väldigt lång tid.
- Ständigt återkommande.
- L0 är förstadiet till en APT.

Vad är APT?
Exempel från verkligheten

- Data skyddat i datorsystem.
- Systemet är helt frånkopplat från alla nätverk.
- Skyddas av låst dörr som kräver passerkort.
- Hur kunde de ta sig igenom?

Vad är APT?
Exempel från verkligheten

- Skicka malware till sekreteraren, avinstallera skrivaren och installera keylogger.
- Sekreteraren kallar in teknikern, teknikern installerar skrivaren.
- Loggar in hos teknikern, beställer nytt passerkort till det säkra rummet.
- Köper upp korttillverkaren, får tillgång till kortet.
- Går rakt in med giltigt passerkort.

Vad är APT?

Future phishermen won't ask you for your mother's maiden name: they'll forge emails from your mother. [And08, s. 50]

Referenser I

[And08] Ross J. Anderson. *Security Engineering*. Wiley, Indianapolis, IN, 2 utgåvan, 2008.

[Clu12] Graham Cluley. The worst passwords you could ever choose exposed by Yahoo Voices hack, 7 2012.

[Duc11] Paul Ducklin. Lost usb keys have 66% chance of malware, 12 2011.

[ER13] Robert Epstein och Ronald E. Robertson. Democracy at risk: Manipulating search rankings can shift voting preferences substatially without voter awareness. Teknisk rapport, American Institute for Behavioural Research and Technology, 2013.

[KSK+11] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Christin Nicolas, Lorrie Faith Cranor och Serge Egelman. Of passwords and people: Measuring the effect of password-composition policies. I: *CHI*, 2011.

Referenser II

[Obe10] Jon Oberheide. Brief analysis of the gawker password dump, 12 2010.

[PHJ+] B. Pan, H. Hembrooke, T. Joachims, L. Lorigo, G. Gay och L. Granka. In Google we trust: Users' decisions on rank, position, and relevance. *Journal of Computer-Mediated Communication*, 12(3).

[TT10] TT. Folk byter lösenord mot choklad. *Dagens Nyheter*, 1 2010.

[xkca] xkcd. Adertising discovery.

[xkcb] xkcd. Password strength.

[xkcc] xkcd. Security.