The Ghosts of Banking Past

Empirical Analysis of Closed Bank Websites

Tyler Moore[1] Richard Clayton[2]

[1] Computer Science and Engineering Department,
Southern Methodist University, Dallas, TX, USA
tylerm@smu.edu
[2] Computer Laboratory, University of Cambridge, UK
richard.clayton@cl.cam.ac.uk

Financial Cryptography and Data Security
Barbados
March 3, 2014

MIVB

Quote

------Jump To-------

Home
About Us
Shareholder Info
Financial Services
Board of Directors
MVB News
Specials
Contact Us

MVB OnLine!

- *Bill Payment*
- *Account Information*
- *Funds Transfers*

Sign Up Sign On

Personal Check Order and Status

You Can now Order new checks ONLINE!

Offshore Bank account

ABOUT US

Safety, Soundness, and Service
People You Can Count On

John B. Dickerson
President & Chief Executive Officer

Since MVB opened its doors in Corning, California, with eight employees in 1975, the bank has been known for its dependability and friendly service. We are now part of a dynamic financial institution serving the communities of Northern California and Southern Oregon from 32 locations. Only one thing has not changed since the very first day - a commitment to provide the best in financial services to individuals and businesses that are the heart of every community. Our Bank maintains relationships with humanitarian and charitable organizations.

Community banking is a business of trust and confidence. The financial services business is always changing...new products and new expectations emerge every day. These and other news from the world of finance, we can find in the section of MVB News. But even after years of change; safety, soundness, and service are still the cornerstones of the MVB business philosophy.

business. We are serious about finding solutions to your house insurance and banking needs. Working together, we can achieve extraordinary results!

Last publications:

New trends in the market of rare earth metals

Send comments or questions to info@midvalleybank.com

business. We are serious about finding solutions to your house insurance and banking needs. Working together, we can achieve extraordinary results!

http://www.canadiancard.ca/
http://www.canadiancard.ca/ - canadiancard.ca has compiled a comprehensive list of visa and mastercards to help people find a credit card card in canada. visit them today to compare reward, low interest, store, student and other credit cards offered by canadian banks and financial institutes.

Last publications:

New trends in the market of rare earth metals

business. We are serious about finding solutions to your house insurance and banking needs. Working together, we can achieve extraordinary results!

http://www.canadiancard.ca/
http://www.canadiancard.ca/ - canadiancard.ca has compiled a comprehensive list of visa and mastercards to help people find a credit card card in canada. visit them today to compare reward, low interest, store, student and other credit cards offered by canadian banks and financial institutes.

MidValley Bank closed in January 2004!

Last publications:

New trends in the market of rare earth metals

Motivation

- The US has thousands of banks, and each year hundreds close through collapse or by acquisition
- While the FDIC has established an orderly process for winding down many bank assets after closure, the websites are often forgotten
- Customers may still try to visit websites after banks have closed, which could lead to confusion
- We set out to measure how prevalent ‘ghost’ banking domains are in practice

Outline

SMU. Bobby B. Lyle School of Engineering

Outline

FDIC data collection

- The FDIC provides an online database of all institutions it has supervised, including those which no longer exist due to merger or collapse
- We focused on 3 181 banks merged or closed between 1 July 2003 and 6 June 2013
- We obtained 2 302 URLs matching 2 393 banks
- For each URL, we fetched WHOIS details and a screenshot of the rendered website

Categorizing bank domain usage

- We manually inspected each of the screenshots and grouped them into one of the following categories
  1. Operable bank-held website (old bank, redirect, or interstitial)
  2. Domain parking pages with syndicated advertisements
  3. Websites used to distribute malware
  4. Other forms of reuse (e.g., blog spam, black-hat SEO)
  5. Inoperable websites (e.g., blank pages, misconfigured websites)
  6. Inactive domains (unregistered, or not resolving)

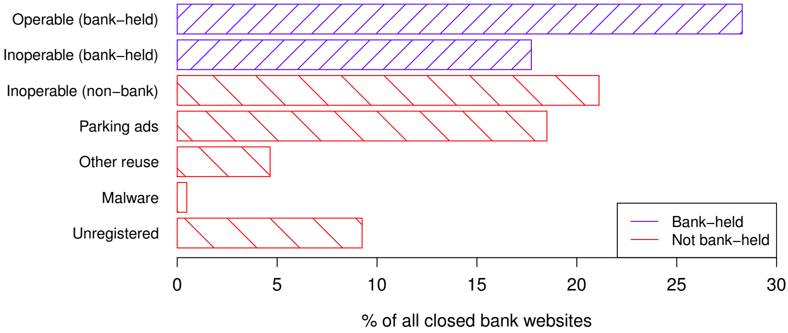
Identifying whether a bank still controls a domain

- We used the following heuristics to confirm that a bank controls a domain
  1. Any website whose screenshot is categorized as a bank *and* the domain has been continuously registered since before the bank closed
  2. Any website that redirects to a currently open bank website URL that appears in the FDIC list
  3. Any domain with WHOIS information indicating ownership by a bank

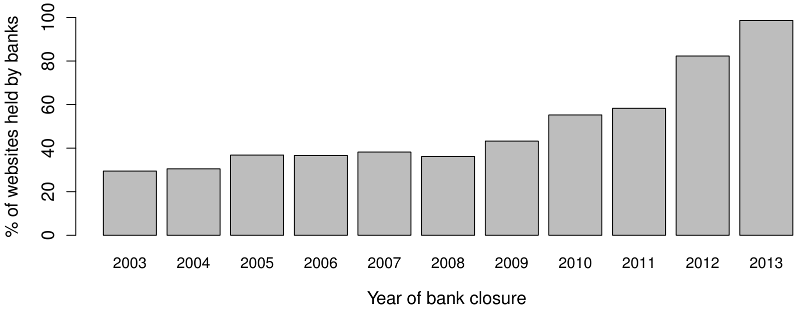
Outline

SMU. Bobby B. Lyle School of Engineering

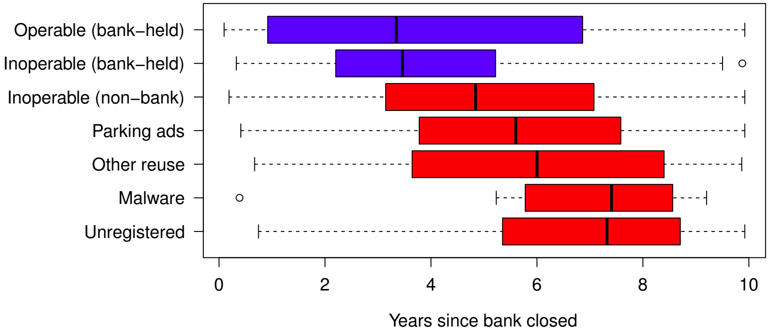
How closed banks are used



Fraction of closed banks whose domains are still owned by a bank, by year of bank closure



Lifecycle of domain reuse



What factors affect the chances a bank domain will be abandoned?

1. **Bank size**
   - Hypothesis: Smaller banks more likely to be abandoned than larger banks
   - Indicator: $\log(\text{Deposits})$
2. **Troubled circumstances at closure**
   - Hypothesis: Troubled banks *more likely* to be abandoned
   - Indicator: Boolean variable set to True if the bank collapsed or was merged with FDIC assistance
3. **Time since closure**
   - Hypothesis: The longer time since a bank has closed, the *more likely* the domain is to be abandoned
   - Indicator: Years since the bank has closed

SMU. Bobby B. Lyle School of Engineering

Logistic regression 1: Factors affecting abandonment

$$\log \frac{p_{abandoned}}{1-p_{abandoned}} = c_0 + c_1 \log(\text{Deposits}) + c_2 \text{ Troubled} + c_3 \text{ Years closed} + $$

Regression 1			Response variable: *Abandoned*	
	coef.	Odds Ratio	95% conf. int.	Significance
(Intercept)	0.58	1.79	(0.90,3.63)	-
log(Deposits)	-0.17	**0.84**	(0.80,0.89)	$p \ll 0.0001$
Troubled	0.87	**2.38**	(1.90,2.98)	$p \ll 0.0001$
Years closed	0.29	**1.33**	(1.29,1.39)	$p \ll 0.0001$
Model fit:	$\chi^2 = 322.8, p \ll 0.0001$			

The resurrection of abandoned bank domains

- 535 bank domains have been allowed to expire at some time after the bank closed
- 326 of these have subsequently been resurrected, that is, re-registered and a new creation date has been recorded in the WHOIS
- We next examine why some domains are resurrected while others aren't

What factors affect the chances an abandoned bank domain will be re-registered?

1. **Bank size**
   - Hypothesis: Larger banks *more likely* to be re-registered
   - Indicator: $\log(\text{Deposits})$
2. **Troubled circumstances at closure**
   - Indicator: Boolean variable set to True if the bank collapsed or was merged with FDIC assistance
3. **Time since closure**
   - Hypothesis: The longer time since a bank has closed, the *less likely* the domain is to be re-registered
   - Indicator: Years since the bank has closed

Logistic regression 2: Factors affecting re-registration

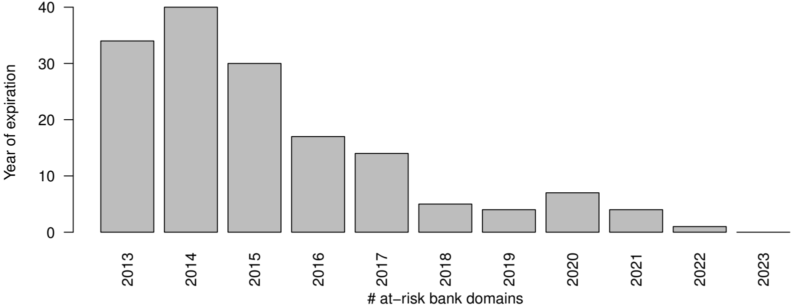
$$\log \frac{p_{registered}}{1 - p_{registered}} = c_0 + c_1 \log(\text{Deposits}) + c_2 \text{ Troubled} + c_3 \text{ Years closed} +$$

Regression 2			Response variable: *Registered*	
	coef.	Odds Ratio	95% conf. int.	Significance
(Intercept)	-0.84	0.43	(0.13,1.38)	-
log(Deposits)	0.33	**1.39**	(1.27,1.53)	$p \ll 0.0001$
Troubled	0.73	**2.08**	(1.18,3.86)	$p = 0.0151$
Years closed	0.24	**0.79**	(0.73,0.85)	$p \ll 0.0001$
Model fit:	$\chi^2 = 120.7, p \ll 0.0001$			

Identifying at-risk bank websites

- We consider a bank-controlled website to be *at-risk* if, according to the WHOIS record, the domain has not been updated since before the bank closed but has yet to expire
- In this circumstance, the bank has not yet had to make a decision whether or not to renew the domain (if they even know there's a decision to be made!)
- 157 of 1 127 bank-controlled websites are at-risk of falling out of bank control

At-risk banks by year of domain expiration



Outline

What is the harm imposed by ghost domains in general?

- Ghost domains are a problem not only for banks
  - At one end, businesses regularly close and domainers are often quick to buy their associated domain names to exploit residual traffic or resell
  - Cybercrime domains (e.g., botnet C&C) are registered to do harm, so their permanent removal seems desirable
  - Banks fall somewhere between, since trust in banking is so crucial to the sector's fiscal health
- We now review a range of mechanisms to reassert control over domains where restrictions over re-registration can be justified

Mechanisms to protect ghost domains

1. **Permanent cancellation**
   - + Avoids any possible harm
   - - Overkill; impractical (and often unwise) to enforce permanence
2. **Prepaid escrow:** certain classes of domains (e.g., banks) must prepay registration fees for many years in the future
   - + Avoids all harm
   - - Only practical in highly-regulated industries
3. **Trusted repository:** neutral body holds domains in trust and decides when and if to reopen a domain to registration
   - - Selecting criteria to release is difficult
   - - Funding could be problematic
4. **Warning lock:** automatic tracking of high-value domains with notification before expiry and volunteers choose whether to defensively register
   - - Selecting criteria to release is difficult
   - - Impact likely extremely patchy

Mechanisms to protect ghost domains

1. **Permanent cancellation**
   - \+ Avoids any possible harm
   - \- Overkill; impractical (and often unwise) to enforce permanence
2. **Prepaid escrow:** certain classes of domains (e.g., banks) must prepay registration fees for many years in the future
   - \+ Avoids all harm
   - \- Only practical in highly-regulated industries
3. **Trusted repository:** neutral body holds domains in trust and decides when and if to reopen a domain to registration
   - \- Selecting criteria to release is difficult
   - \- Funding could be problematic
4. **Warning lock:** automatic tracking of high-value domains with notification before expiry and volunteers choose whether to defensively register
   - \- Selecting criteria to release is difficult
   - \- Impact likely extremely patchy

SMU. Bobby B. Lyle School of Engineering

Mechanisms to protect ghost domains

1. **Permanent cancellation**
   + Avoids any possible harm
   - Overkill; impractical (and often unwise) to enforce permanence
2. **Prepaid escrow:** certain classes of domains (e.g., banks) must prepay registration fees for many years in the future
   + Avoids all harm
   - Only practical in highly-regulated industries
3. **Trusted repository:** neutral body holds domains in trust and decides when and if to reopen a domain to registration
   - Selecting criteria to release is difficult
   - Funding could be problematic
4. **Warning lock:** automatic tracking of high-value domains with notification before expiry and volunteers choose whether to defensively register
   - Selecting criteria to release is difficult
   - Impact likely extremely patchy

Mechanisms to protect ghost domains

1. **Permanent cancellation**
   - + Avoids any possible harm
   - - Overkill; impractical (and often unwise) to enforce permanence
2. **Prepaid escrow:** certain classes of domains (e.g., banks) must prepay registration fees for many years in the future
   - + Avoids all harm
   - - Only practical in highly-regulated industries
3. **Trusted repository:** neutral body holds domains in trust and decides when and if to reopen a domain to registration
   - - Selecting criteria to release is difficult
   - - Funding could be problematic
4. **Warning lock:** automatic tracking of high-value domains with notification before expiry and volunteers choose whether to defensively register
   - - Selecting criteria to release is difficult
   - - Impact likely extremely patchy

SMU. Bobby B. Lyle School of Engineering

Conclusions

- When banks close, their domains are often forgotten: 53% of domains for US banks closed in the past decade are no longer controlled by banks
- This can create confusion for consumers and opportunities for cybercriminals
- Regression analysis has shown that smaller or troubled banks are more likely to abandon domains, while larger and more recently closed banks are more likely to be re-registered
- We recommend that bank regulators help coordinate the defensive registration of at-risk domains
- For more: `http://lyle.smu.edu/~tylerm/`

SMU. Bobby B. Lyle School of Engineering